LANTRONIX®

PremierWave® XN
Command Reference

Part Number 900-607
Revision A February 2012

Copyright and Trademark

© 2012 Lantronix. All rights reserved. No part of the contents of this book may be transmitted or reproduced in any form or by any means without the written permission of Lantronix. Printed in the United States of America.

Ethernet is a trademark of XEROX Corporation. Windows is a trademark of the Microsoft Corporation.

Contacts

Lantronix Corporate Headquarters

167 Technology Drive
Irvine, CA 92618, USA
Toll Free: 800-526-8766
Phone: 949-453-3990
Fax: 949-450-7249

Technical Support

Online: www.lantronix.com/support

Sales Offices

For a current list of our domestic and international sales offices, go to the Lantronix web site at www.lantronix.com/about/contact.

Disclaimer

The information in this guide may change without notice. The manufacturer assumes no responsibility for any errors that may appear in this guide.

Revision History

Date	Revision	Comments
February 2012	A	Initial Document. Created for the 7.3.0.0 release.

Table of Contents

List of Figures ____ 4
List of Tables ____ 5

1: About This Guide 6

Chapter Summaries ____ 6
Conventions ____ 6
Additional Documentation ____ 7

2: Overview 8

XML Architecture and Device Control ____ 8
Command Line Interface ____ 8

3: Command Line Interface 9

Configuration Using Telnet ____ 9
Configuration Using Serial Ports ____ 9
Serial Command Mode ____ 9
Serial Recovery ____ 9
Navigating the CLI Hierarchy ____ 10
Using Keyboard Shortcuts and CLI ____ 11
Understanding the CLI Level Hierarchy ____ 11

4: Configuration Using XML 14

XML Configuration Record Document Type Definition ____ 14
Quick Tour of XML Syntax ____ 15
Declaration ____ 15
Element Start and End Tags ____ 15
Element Attributes ____ 15
Record, Group, Item, and Value Tags ____ 16
Importing and Exporting an XML Configuration File ____ 17
Best Practices ____ 18
Importing ____ 18
Exporting ____ 19
XML Configuration Groups ____ 20
XML Status Record Groups and Items ____ 33

5: Command and Levels 44

List of Figures

Figure 3-2 CLI Level Hierarchy 12
Figure 3-3 Login Level Commands 12
Figure 3-4 Enable Level Commands 13
Figure 4-1 DTD for XCRs 14
Figure 4-2 XML Example 15
Figure 4-3 XML Example 16
Figure 4-4 XML Example of Multiple Named Values 16
Figure 4-5 XML Example of Multiple Items 17
Figure 4-6 XML Example with Multiple Groups 17

List of Tables

Table 3-1 Keyboard Shortcuts _____ 11
Table 4-7 XCR Groups _____ 20
Table 4-8 XSR Group and Items _____ 33
Table 5-1 Commands and Levels _____ 47

1: About This Guide

This guide describes how to configure the PremierWave XN using the Command Line Interface (CLI) and/or Extensible Markup Language (XML). It is written for software developers and system integrators.

Chapter Summaries

This table lists and summarizes content of each chapter.

Chapter	Summary
Chapter 2: Overview	Gives an overview of CLI and XML.
Chapter 3: Command Line Interface	Lists commands and describes how to use CLI to configure the PremierWave XN.
Chapter 4: Configuration Using XML	Lists XCR groups and items and describes how to use XCRs to configure the PremierWave XN.
Chapter 5: Commands and Levels	Provides an index of the CLI Command Hierarchy with hyperlinks to the corresponding command details.

Conventions

The table below lists and describes the conventions used in this book.

Convention	Description
Bold text	Default parameters.
Italic text	Required values for parameters
Brackets [ ]	Optional parameters.
Angle Brackets < >	Possible values for parameters.
Pipe |	Choice of parameters.
Warning	***Warning:*** ***Means that you are in a situation that could cause equipment damage or bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and familiar with standard practices for preventing accidents.***
Note	***Note:*** *Means take notice. Notes contain helpful suggestions, information, or references to material not covered in the publication.*
Caution	***Caution:*** ***Means you might do something that could result in faulty equipment operation, or loss of data.***
Screen Font (Courier New)	`CLI terminal sessions and examples of CLI input.`

Additional Documentation

Visit the Lantronix website at www.lantronix.com/support/documentation for the latest documentation and the following additional documentation.

Document	Description
PremierWave XN User Guide	Describes how to configure and use the PremierWave XN.
PremierWave XN Quick Start Guide	Instructions for getting the PremierWave XN up and running.
Com Port Redirector Quick Start and Online Help	Instructions for using the Lantronix Windows-based utility to create virtual com ports.
DeviceInstaller Online Help	Instructions for using the Lantronix Windows-based utility to locate the PremierWave XN and to view its current settings.

2: Overview

PremierWave XN supports three convenient configuration methods: Web Manager, Command Line Interface (CLI) and Extensible Markup Language (XML). For more information about the Web Manager, see the *PremierWave* XN *User Guide* on the Lantronix website.

XML Architecture and Device Control

XML is a fundamental building block for the future growth of Machine-to-Machine (M2M) networks. PremierWave supports XML configuration records that make configuring the device server easy for users and administrators. XML configuration records are easy to edit with a a standard text editor or an XML editor.

For a brief overview of XML, see *Chapter 4: Configuration Using XML*. It provides rules on basic XML syntax, a guide to the specific XML tags used, and a guide to using XML configuration records.

Command Line Interface

Making the edge-to-enterprise vision a reality, PremierWave XN uses industry-standard tools for configuration, communication, and control. For example, the PremierWave XN uses a command line interface (CLI) whose syntax is very similar to that used by data center equipment such as routers and hubs.

For details of the CLI, see *Chapter 5: Commands and Levels*. It provides an index of the CLI Command Hierarchy with links to the corresponding command details. The CLI provides commands for configuring, monitoring, and controlling the device server.

3: Command Line Interface

This chapter describes accessing the PremierWave XN by using Telnet, SSH, or serial ports to configure the PremierWave XN, navigating the Command Line Interface (CLI), typing keyboard shortcuts, and moving between the levels.

It contains the following sections:

- *Configuration Using Telnet*
- *Configuration Using Serial Ports*
- *Navigating the CLI Hierarchy*
- *Using Keyboard Shortcuts and CLI*
- *Understanding the CLI Level Hierarchy*

Refer to *Chapter 5: Commands and Levels* for a complete list of levels, commands, and descriptions.

Configuration Using Telnet

To access and configure the device server by using a Telnet session over the network, you must first establish a Telnet connection. You can also establish a Telnet connection by clicking the Telnet Configuration tab in DeviceInstaller. See the DeviceInstaller Online Help for more information, available on our website www.lantronix.com/support/downloads.

To access the PremierWave XN by using Telnet, perform the following steps.

1. Click **Start > Run**. The Run dialog box displays.
2. Type `cmd` in the dialog box and press **OK**.
3. Type `telnet x.x.x.x` (x.x.x.x is the IP address). The PremierWave XN is online when the command prompt (>) displays. You are at the root level of the CLI.

Note: *Depending on the level of security, a password may be required.*

Configuration Using Serial Ports

Serial Command Mode

The serial port can be configured to operate in command mode permanently or to be triggered under specified conditions. See the `line <line> Level` command description for more information.

Serial Recovery

Serial Recovery mode will temporarily override the line and tunnel settings for the serial line to allow configuration changes to be made. The line and tunnel settings will be restored once the user exits the Serial Recovery mode CLI.

To configure the Lantronix device server locally using a serial port:

1. Connect a terminal or a PC running a terminal emulation program to one of the device server's serial ports.
2. Configure the terminal to the following settings:
   - 9600 baud
   - 8-bit
   - No parity
   - 1 stop bit
   - No flow control.
3. Power off the device.
4. Press and hold down the exclamation point (`!`) key.
5. Power on the device. After about 10 seconds, the exclamation point will display on the terminal or PC screen.
6. Type `xyz` within 5 seconds to display the CLI prompt.

Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of levels. Each level has a group of commands for a specific purpose. For example, to configure a setting for the FTP server, one would navigate to the FTP level, which is under the configuration level.

- To move to a different level—Enter the name of the level from within its parent level. For example, to enter the tunnel level, type `tunnel <number>` at the enable prompt. This displays: `<enable> tunnel <number>#`.
- To exit and return to one level higher—Type `exit` and press the **Enter** key. Typing exit at the login level or the enable level will close the CLI session. If Line - Command Mode is specified as Always, a new session starts immediately.
- To view the current configuration at any level—Type `show`.
- To view the list of commands available at the current level—Type the question mark "`?`". Items within `< >` (e.g. `<string>`) are required parameters.
- To view the available commands and explanations—Type the asterisk (`*`).
- To view the list of commands available for a partial command—Type the partial command followed by the question mark "`?`". For example: `<tunnel-1>#echo?` displays a list of all echo commands at the tunnel level.
- To view available commands and their explanations for a partial command—Type the partial command followed by the asterisk (`*`). For example: `<tunnel-1>#echo*` displays a list of all echo commands and descriptions at the tunnel level.
- To view the last 20 commands entered at the CLI—Type `show history`.

Using Keyboard Shortcuts and CLI

One useful shortcut built into PremierWave XN is that the complete text of a command does not have to be entered to issue a command. Typing just enough characters to uniquely identify a command, then hitting enter, can be used as a short cut for a command. For example, at the enable level, "`sh`" can be used for the "`show`" command.

Tab Completion is also available using the **Tab** and **Enter** keys on the keyboard. Typing the first few characters of a command, then hitting the **Tab** key displays the first command that begins with those characters. Hitting the **Tab** key again displays the next command that begins with the original characters typed. You can press **Enter** to execute the command or you can backspace to edit any parameters.

The following key combinations are allowed when configuring the device server using the CLI:

Table 3-1 Keyboard Shortcuts

Key Combination	Description
Ctrl + a	Places cursor at the beginning of a line
Ctrl + b	Backspaces one character
Ctrl + d	Deletes one character
Ctrl + e	Places cursor at the end of the line
Ctrl + f	Moves cursor forward one character
Ctrl + k	Deletes from the current position to the end of the line
Ctrl + l	Redraws the command line
Ctrl + n	Displays the next line in the history
Ctrl + p	Displays the previous line in the history
Ctrl + u	Deletes entire line and places cursor at start of prompt
Ctrl + w	Deletes one word back
Ctrl + z	Exits the current CLI level
Esc + b	Moves cursor back one word
Esc + f	Moves cursor forward one word

Understanding the CLI Level Hierarchy

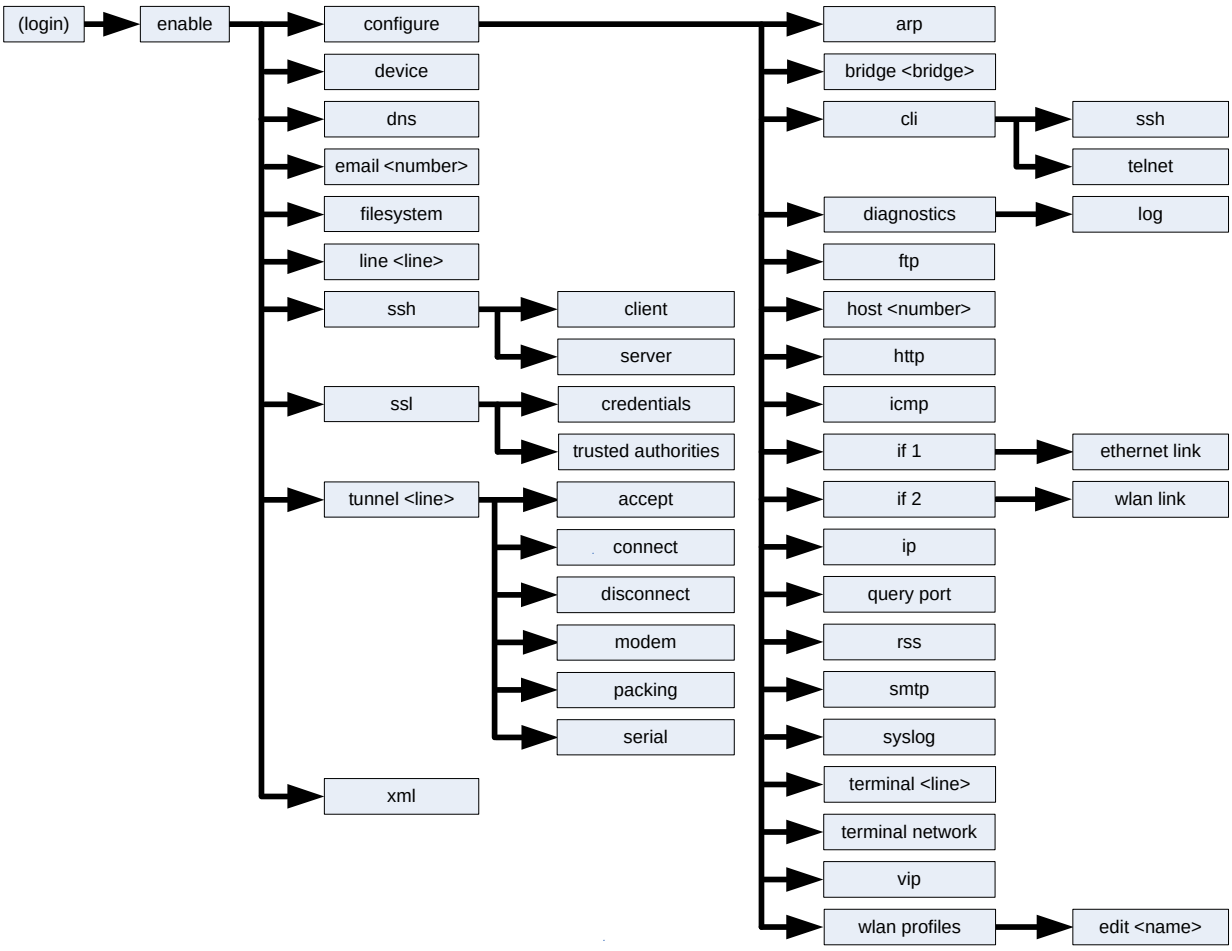
The CLI hierarchy is a series of levels. Arranging commands in a hierarchy of levels provides a way to organize and group similar commands, provide different levels of security, and reduce the complexity and number commands and options presented to a user at one time.

When you start a command line session, you begin at the login level. This level can be password protected and provides access to high level status, a few diagnostic commands, and the enable level. Further device information and configuration are accessed via the enable level.

The enable level can also be password protected and is the gateway to full configuration and management of the device server. There are commands for gathering and effecting all elements of device status and configuration, as well as commands that take you to additional levels. For instance, tunnel specific status and configuration is found under the "tunnel" level, and network specific status and configuration commands are found under the "configuration" level.

An overview of the levels in the PremierWave XN is presented in *Figure 3-2 CLI Level Hierarchy* below.

Figure 3-2 CLI Level Hierarchy



Commands at the login level (see *Figure 3-3 Login Level Commands* below) do not affect current configuration settings and are not displayed initially. If you type `?`, you will see the login sub-commands. These commands provide diagnostic and status information only.

Figure 3-3 Login Level Commands

```
>?
clrscrn                                  exit
ping <host>                              ping <host> <count>
ping <host> <count> <timeout>            show
show history                             trace route <host>
trace route <host> <protocol>            enable
>
```

Note: *To configure the PremierWave XN, you must be in the enable level and any of its sub-levels. Figure 3-4 below shows the enable level commands.*

Figure 3-4 Enable Level Commands

```
>enable
<enable>#?
auto show interfaces                          auto show processes
clrscrn                                       configure
connect                                       connect line <line>
device                                        disable
dns                                           email <number>
exit                                          filesystem
kill ssh <session>                            kill telnet <session>
line <line>                                   ping <host>
ping <host> <count>                           ping <host> <count> <timeout>
reload                                        reload factory defaults
show                                          show history
show interfaces                               show ip sockets
show processes                                show sessions
ssh                                           ssh <optClientUsername> <host>
ssh <optClientUsername> <host> <port>         ssl
telnet <host>                                 telnet <host> <port>
trace route <host>                            trace route <host> <protocol>
tunnel <line>                                 write
xml

<enable>#_
```

See the *Chapter 5: Commands and Levels* at the end of this document for a complete list of levels, commands, and descriptions.

4: Configuration Using XML

The device server provides an Extensible Markup Language (XML) interface that you can use to configure device server devices. Every configuration setting that can be issued from the device server Web Manager and CLI can be specified using XML.

The device server can import and export configuration settings as an XML document known as an XML Configuration Record (XCR). An XCR can be imported or exported via the CLI, a Web browser, FTP, or the device server filesystem. An XCR can contain many configuration settings or just a few. For example, it might change all of the configurable parameters for a device server, or it may only change the baud rate for a single serial line. Using XCRs is a straightforward and flexible way to manage the configuration of multiple device server devices.

XML Configuration Record Document Type Definition

An XML document type definition (DTD) is a description of the structure and content of an XML document. It verifies that a document is valid. XCRs are exported using the DTD as shown in *Figure 4-1 DTD for XCRs*.

Figure 4-1 DTD for XCRs

```
<!DOCTYPE configrecord [
<!ELEMENT configrecord (configgroup+)>
<!ELEMENT configgroup (configitem+)>
<!ELEMENT configitem (value+)>
<!ELEMENT value (#PCDATA)>
<!ATTLIST configrecord version CDATA #IMPLIED>
<!ATTLIST configgroup name CDATA #IMPLIED>
<!ATTLIST configgroup instance CDATA #IMPLIED>
<!ATTLIST configitem name CDATA #IMPLIED>
<!ATTLIST value name CDATA #IMPLIED>
]>
```

The device server DTD rules state the following:

- The XML document element is a `<configrecord>` element. This is the root element.
- A `<configrecord>` must have one or more `<configgroup>` elements and can have a version attribute.
- A `<configgroup>` must have one or more `<configitem>` elements and can have name and instance attributes.
- A `<configitem>` element must have one or more <value> elements and can have a name attribute.
- A `<value>` element can have only data and can have a name attribute.
- The name attribute identifies a group, item, or value. It is always a quoted string.
- The instance attribute identifies the specific option, like the serial port number. The "instance" attribute is always a quoted string.

Note:

- *The name for each <configgroup> (specified with the name attribute) is the group name listed in the Web Manager XCR groups or with the "xcr list" CLI command. See the PremierWave XN User Guide for more information about the XCR groups.*
- *An empty or missing <value> element in each present <configgroup> clears the setting to its default.*

Quick Tour of XML Syntax

Declaration

The first line, `<?xml version="1.0" standalone="yes"?>`, is called the XML declaration. It is required and indicates the XML version in use (normally version 1.0). The remainder of the file consists of nested XML elements, some of which have attributes and content.

Element Start and End Tags

An element typically consists of two tags: start tag and an end tag that surrounds text and other elements (element content). The start tag consists of a name surrounded by angle brackets, for example `<configrecord>`. The end tag consists of the same name surrounded by angle brackets, but with a forward slash preceding the name, for example `</configrecord>`. The element content can also contain other "child" elements.

Element Attributes

The XML element attributes that are name-value pairs included in the start tag after the element name. The values must always be quoted, using single or double quotes. Each attribute name should appear only once in an element.

XML Example shows an XML example which consists of a declaration (first line), nested elements with attributes and content.

Figure 4-2 XML Example

```
<?xml version=”1.0” standalone=”yes”?>
<configrecord>
<configgroup name = “serial command mode” instance = “1”>
<configitem name = “mode serial string”>
<value>disable</value>
</configitem>
</configgroup>
</configrecord>
```

The PremierWave XN uses the attributes in the following subsections to label the group configuration settings.

Record, Group, Item, and Value Tags

A <configgroup> is a logical grouping of configuration parameters and must contain one or more <configitem> elements. It must have a name attribute and may have an instance attribute.

A <configitem> is a specific grouping of configuration parameters relevant to its parent group. An item takes the name attribute and must contain one or more value elements. For example, the line group might have parameters such as baud rate, data bits, and parity.

A value may specify the value of a configuration parameter. It may contain the name attribute. In this example, a value of 9600 might be specified for baud rate; 7 may be specified for data bits, and even may be specified for parity.

A name attribute identifies the group, item, or value. It is always quoted (as are all XML attributes). For example, a group that contains serial port parameters has the name "line".

An instance attribute identifies which of several instances is being addressed. It is always quoted. For example, the serial port name (in the line configgroup) has the instance "1" to indicate serial port 1 or "2" to specify serial port 2.

The following figures show examples of XML configuration records and the use of the <configrecord>, <configgroup>, <configitem>, and <value> XML elements.

Figure 4-3 XML Example

```
<?xml version="1.0" standalone="yes"?>
<configrecord>
<configgroup name = "serial command mode" instance = "1">
<configitem name = "mode">
<value>disable</value>
</configitem>
</configgroup>
</configrecord>
```

Figure 4-4 XML Example of Multiple Named Values

```
<?xml version="1.0" standalone="yes"?>
   <configgroup name = "ethernet" instance = "eth0">
       <configitem name = "speed">
           <value>Auto</value>
       </configitem>
       <configitem name = "duplex">
           <value>Auto</value>
       </configitem>
   </configgroup>
```

Figure 4-5 XML Example of Multiple Items

```
<configgroup name="ssh server">
      <configitem name="host rsa keys">
        <value name="public key"/>
        <value name="private key"/>
  </configitem>
      <configitem name="host dsa keys">
        <value name="public key"/>
        <value name="private key"/>
  </configitem>
      <configitem name="delete authorized users">
       <value>disable</value>
  </configitem>
      <configitem name="authorized user delete">
       <value name="name"/>
  </configitem>
      <configitem name="authorized user" instance="">
       <value name="password"/>
       <value name="public rsa key"/>
       <value name="public dsa key"/>
  </configitem>
</configgroup>
```

Figure 4-6 XML Example with Multiple Groups

```
<?xml version="1.0" standalone="yes"?>
   <configgroup name = "telnet">
       <configitem name = "state">
           <value>enable</value>
       </configitem>
       <configitem name = "authentication">
           <value>disable</value>
       </configitem>
   </configgroup>
   <configgroup name = "ssh">
       <configitem name = "state">
           <value>enable</value>
       </configitem>
   </configgroup>
```

Importing and Exporting an XML Configuration File

An XCR can be imported or exported using the following methods:

- Filesystem-XCRs can be saved to the device server file system and imported or accessed as needed. See *Best Practices on page 18* or the Filesystem Browser section in the *PremierWave XN User Guide*.

- CLI-XCRs can be imported (captured) or exported (dumped) directly to a Telnet, SSH, or serial line CLI session. Capturing an XCR can be started by pasting a valid XCR directly into the CLI prompt. PremierWave XN immediately processes the configuration record, changing any settings specified. This can be done on any level, including the root. Special tags in the XML allow for providing root and enable level passwords so that this can also be done at the password prompt.
- Web browser-Web Manager can be used to import and export an XCR to the device server file system. It can also be used to import an XCR from an external source such as your local hard drive.
- FTP-The device server FTP server can export and import XCRs when an FTP get or put command on the filename (pwxn.xcr for export, pwxn_import.xcr for import; both are under the pwxcr directory) is requested. On export (FTP get of pwxn.xcr), the FTP server obtains the current XCR from the PremierWave XN and sends it as a file. On import (FTP put of pwxn_import.xcr), the FTP server processes the file by sending it directly to the XML engine. In both cases the device server filesystem is not accessed. The files pwxn.xcr and pwxn_import.xcr are not read from or written to the file system. See FTP in the *PremierWave XN User Guide*.

Best Practices

You can import or export an entire XCR, or just a portion of it, by specifying the group name and/or group instances. In the examples below, import and export operations are performed from the CLI on the local filesystem and require a XCR on the local filesystem. The Web Manager provides the same functionality.

Caution: ***Using Microsoft Word to edit and save an XCR will change the format of the file and make it incompatible with PremierWave XN. This is true even if the file is saved as Plain Text (.txt) or an XML Document (.xml). Notepad, a third party text editor, or a specialized XML editor should be used instead.***

Importing

The following syntax can be used to import configurations from a file:

```
xcr import <file>
xcr import <file> <groups and/or group:instances>
```

The first line imports all groups specified in the XML config record named in <file>. Any filename is valid, and the file name and extension are not important.

In the second line:

- Instance follows group with a colon (see the third example on the next page).
- Multiple groups are separated with a comma.
- Any white space requires the list of groups to be quoted.
- Only the named groups get imported, even if the XCR contains additional XCR groups.

The following syntax can be used to export configurations to a file on the device server's file system:

```
xcr export <file>
xcr export <file> <groups and/or group:instances>
```

The same guidelines above regarding importing configurations also apply to exporting configurations. If no groups are specified, then the export command will export all configuration settings to the file. If instances are specified after the groups, only those group instances are written. If no instance is specified, all instances of that group are written.

Exporting

The following example exports only the accept mode tunneling settings for line 1 to the file "tunnel_1.xcr" on the device server filesystem:

```
xcr export tunnel_1.xcr "tunnel accept:1"
```

The following example exports only the connect mode tunneling settings for all ports to the file "tunnel_all.xcr" on the device server filesystem:

```
xcr export tunnel_all.xcr "tunnel connect"
```

The following example imports only the settings for line 2 from a XCR named "factory_config.xcr" on the device server filesystem. If "factory_config.xcr" has other configuration settings, they are ignored:

```
xcr import factory_config.xcr "line:2"
```

The following example imports only line settings for all ports from a configuration record on the device server filesystem named "foobar.xcr":

```
xcr import foobar.xcr "line"
```

To import only disconnect mode tunneling settings for port 1 and serial line settings for port 2 from an XML configuration record named "production.xcr" that contains these settings (and possibly more), issue the following command:

```
xcr import production.xcr "tunnel disconnect:1, line:2"
```

The following example imports all tunneling settings and line settings for all serial ports from a file named xcr_file:

```
xcr import xcr_file "tunnel accept, tunnel connect, tunnel
disconnect, tunnel modem, tunnel packing, tunnel serial, tunnel
start, tunnel stop, line"
```

The following example exports only accept mode tunneling settings on serial port 1, and line settings on serial port 2 to a file named tunnel_config_t1_l2.xcr on the device server filesystem.

```
xcr export tunnel_config_t1_l2.xcr "tunnel accept:1, line:2"
```

The following example exports connect mode tunneling and line settings for all ports to the file tunnel_config.xcr on the device server filesystem:

```
xcr export tunnel_config.xcr "tunnel, line"
```

XML Configuration Groups

Table 4-7 lists the PremierWave XN XCR groups in alphabetical order. This table indicates the various group items, as well as some possible value names and options.

Note: *Any instance of **&#60** in the table may be read as "less than" and any instance of **&#62** may be read as "greater than".*

Table 4-7 XCR Groups

Group Name	Group Item	Value Name	Value Options	Additional Information
arp	arp delete	ip address		Remove an entry from the ARP table. Specify the entry by its IP address.
	arp entry	ip address		
		mac address		
bridge	state		enable, disable	Default: disable
	bridging mac address			
cli	login password			Value is SECRET, hidden from user view. Default: PASS
	enable level password			Value is SECRET, hidden from user view.
	quit connect line			Accepts text containing control characters, for example, <control>A represents control-A Default: <control>L
	inactivity timeout		<None>, ...	Default: 15 minutes
	line authentication		enable, disable	Default: disable
device	short name			
	long name			
	serial number			Read only.
	firmware version			Read only.
diagnostics	log	output	disable, filesystem, line <number>	Default: disable
		max length		Default: 50 KB
email	to			
	cc			
	from			
	reply to			

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
email (continued)	subject			
	message file			
	overriding domain			
	server port			Default: 25
	local port		<Random>, ...	Default: <Random>
	priority		urgent, high, normal, low, very low	Default: normal
ethernet	speed		auto, 10, 100	Default: auto
	duplex		auto, half, full	Default: auto
ftp server	state			
host	name			
	protocol		telnet, ssh	Default: telnet
	ssh username			
	remote address			
	remote port			Default: 0
http authentication uri	user delete	name		Deletes an HTTP Authentication URI user. The value element is used to specify the user for deletion.
	realm			
	type			
	user	password		
http server	state		enable, disable	Default: enable
	port		<None>, ...	Default: 80
	secure port		<None>, ...	Default: 443
	secure protocols		ssl3, tls1.0, tls1.1	May contain zero, one, or more of the values, separated by commas. Default: ssl3, tls1.0, tls1.1
	secure credentials			
	max timeout			Default: 10 seconds
	max bytes			Default: 40960
	logging state		enable, disable	Default: enable
	max log entries			Default: 50
	log format			Default: %h %t "%r" %s %B "%{Referer}i" "%{User-Agent}i"
	authentication timeout			Default: 30 minutes

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
icmp	state		enable, disable	Default: enable
interface	state		enable, disable	Default: depends on instance
	bootp		enable, disable	Default: disable
	dhcp		enable, disable	Default: enable
	ip address		<None>, ...	Accepts an IP address and mask as either: (1) IP address only (192.168.1.1) gets a default mask, (2) CIDR (192.168.1.1/24), or (3) Explicit mask (192.168.1.1 255.255.255.0).
	default gateway		<None>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	hostname			
	domain			
	dhcp client id			
	primary dns		<None>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	secondary dns		<None>, ...	Accepts in IP address in dotted notation, like 192.168.1.1.
	mtu			Default: 1500 bytes
ip	ip time to live			Default: 64 hops
	multicast time to live			Default: 1 hops

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
line	name			
	interface		rs232	Default:
	termination		enable, disable	Default: disable
	state		enable, disable	Default: depends on instance
	protocol		none, tunnel	Default:
	baud rate			Default: 9600 bits per second
	parity		even, none, odd	Default: none
	data bits		7, 8	Default: 8
	stop bits		1, 2	Default: 1
	flow control		none, hardware, software	Default: none
	xon char			Accepts a control character, for example, <control>A represents control-A Default: <control>Q
	xoff char			Accepts a control character, for example, <control>A represents control-A Default: <control>S
	gap timer		<None>, ...	Default: <None>
	threshold			Default: 56 bytes

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
managelinx	plaintext dsm credentials	dna.xml.replication.protocol.version		
		dna.capabilities.tcp.connect.fail	enable, disable	Default: disable
	encrypted dsm credentials	dna.dsc.auth.tunnel.username		
		dna.dsc.auth.ssh.pub		
		dna.dsc.auth.ssh.priv		
		device.dna.dsc.tunnel.portlist.list		
		device.dna.dsc.tunnel.ip.addr		
		device.dna.dsc.tunnel.ip.list		
		device.dna.dsc.tunnel.ssh.public		
		device.dnaid		
		device.dna.dsc.tunnel.portlist.httpconnect		
		device.dna.dsc.tunnel.proxy.host		
		device.dna.dsc.tunnel.proxy.port		
		device.dna.dsc.tunnel.proxy.enable		
	managelinx common	device.dna.system.change.number		
		device.config.name		
		device.dna.system.change.timestamp		
		device.dna.dsc.replication.period		Default: 1800 seconds
	managelinx network interface	device.dna.system.network.iface.name		
		device.dna.system.network.iface.ipaddress		
		device.dna.system.network.iface.vip.pool		Default: 0
		device.viproute.target.name		
query port	state		enable, disable	Default: enable
rss	feed		enable, disable	Default: disable
	persist		enable, disable	Default: disable
	max entries			Default: 100

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
serial command mode	mode		always, serial string, disable	Default: disable
	echo serial string		enable, disable	Default: enable
	serial string			Sets a string that can be entered at boot time to enter command mode. This text may specify binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
	signon message			Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode. This text may specify binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
	wait time			Default: 5000 milliseconds
smtp	relay address			
	relay port			Default: 25
ssh	state		enable, disable	Default: enable
	port			Default: 22
	max sessions			Default: 3

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
ssh client	delete known hosts		enable, disable	If enabled, deletes any existing hosts before adding "known host".
	known host delete	name		Specify the known host to delete.
	known host	public rsa key		
		public dsa key		
	delete client users		enable, disable	If enabled, deletes any existing client users before adding "client user".
	client user delete	name		Specify the user to delete.
	client user	password		
		remote command		
		public rsa key		
		private rsa key		
		public dsa key		
		private dsa key		
ssh server	host rsa keys	public key		
		private key		
	host dsa keys	public key		
		private key		
	delete authorized users			
	authorized user delete	name		
	authorized user	password		
		public rsa key		
		public dsa key		

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
ssl	credentials	rsa certificate		
		rsa private key		Value is SECRET, hidden from user view.
		dsa certificate		
		dsa private key		Value is SECRET, hidden from user view.
	trusted authority	certificate		
	intermediate authority	certificate		
	delete all credentials		enable, disable	If enabled, deletes any existing credentials before adding "credentials".
	delete all cas		enable, disable	If enabled, deletes any existing trusted cas before adding "trusted ca".
syslog	state		enable, disable	Default: disable
	host			
	remote port			Default: 514
	severity log level		none, emergency, alert, critical, error, warning, notice, information, debug	Default: none
telnet	state		enable, disable	Default: enable
	port			Default: 23
	max sessions			Default: 3
	authentication		enable, disable	Default: disable
terminal	terminal type			Default: UNKNOWN
	login connect menu		enable, disable	Default: disable
	exit connect menu		enable, disable	Default: disable
	send break			Accepts a control character, for example, <control>A represents control-A
	break duration			Default: 500 milliseconds
	echo		enable, disable	Default: enable
tunnel accept	accept mode		disable, always, any character, start character, modem control asserted, modem emulation	Default: always

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel accept (continued)	start character			Accepts a control character, for example, <control>A represents control-A Default: <control>B
	flush start character		enable, disable	Default: enable
	local port			Default: 0
	protocol		tcp, ssh, telnet, tcp aes, ssl	Default: tcp
	credentials			
	tcp keep alive		<None>, ...	Default: 45000 milliseconds
	aes encrypt key			Value is SECRET, hidden from user view.
	aes decrypt key			Value is SECRET, hidden from user view.
	flush serial		enable, disable	Default: disable
	block serial		enable, disable	Default: disable
	block network		enable, disable	Default: disable
	password	password		Value is SECRET, hidden from user view.
		prompt	enable, disable	Default: disable
	email connect		<None>, ...	Default: <None>
	email disconnect		<None>, ...	Default: <None>
tunnel connect	connect mode		disable, always, any character, start character, modem control asserted, modem emulation	Default: disable
	start character			Accepts a control character, for example, <control>A represents control-A Default: <control>B
	flush start character		enable, disable	Default: enable
	local port		<Random>, ...	Default: <Random>

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel connect (continued)	host	vip	enable, disable	Default: disable
		vip name		
		address		
		port	<None>, ...	Default: <None>
		protocol	tcp, udp, ssh, telnet, tcp aes, udp aes, ssl	Default: tcp
		ssh username		
		credentials		
		validate certificate	enable, disable	Default: enable
		tcp keep alive	<None>, ...	Default: 45000 milliseconds
		aes encrypt key		Value is SECRET, hidden from user view.
		aes decrypt key		Value is SECRET, hidden from user view.
	host mode		sequential, simultaneous	Default: sequential
	reconnect time			Default: 15000 milliseconds
	flush serial		enable, disable	Default: disable
	block serial		enable, disable	Default: disable
	block network		enable, disable	Default: disable
	email connect		<None>, ...	Default: <None>
	email disconnect		<None>, ...	Default: <None>
tunnel disconnect	stop character			Accepts a control character, for example, <control>A represents control-A
	flush stop character		enable, disable	Default: enable
	modem control		enable, disable	Default: disable
	timeout			Default: 0 milliseconds
	flush serial		enable, disable	Default: disable
tunnel modem	echo pluses		enable, disable	Default: disable
	echo commands		enable, disable	Default: enable
	verbose response		enable, disable	Default: enable
	response type		text, numeric	Default: text
	error unknown commands		enable, disable	Default: disable
	incoming connection		disabled, automatic, manual	Default: disabled
	connect string			
	display remote ip		enable, disable	Default: disable

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
tunnel packing	packing mode		disable, timeout, send character	Default: disable
	timeout			Default: 1000 milliseconds
	threshold			Default: 512 bytes
	send character			Accepts a control character, for example, <control>A represents control-A Default: <control> M
	trailing character			Accepts a control character, for example, <control>A represents control-A
tunnel serial	dtr		asserted while connected, continuously asserted, unasserted, truport	Default: asserted while connected
vip	state		enable, disable	Default: disable
wlan	choice	profile		
	debugging level		dump, debug, info, warning, error	Default: info
	active channel scan time			Default: 100 milliseconds
	passive channel scan time			Default: 400 milliseconds
	radio band selection		2.4 ghz only, 5 ghz only, dual	Default: dual
	out of range scan interval		10 - 30 seconds	Default: 30 seconds
	roaming		enable, disable	Default: disabled
	rssi delta		14 - 24dBm	Default: 24dBm
wlan profile	basic	network name		
		topology	infrastructure, adhoc	Default: infrastructure
		scan 2.4 ghz band	enable, disable	Default: enable
		scan 5 ghz band	enable, disable	Default: enable
		scan dfs channels	enable, disable	Default: enable
		state	enable, disable	Enables or disables the profile.
		channel		Default: 1

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
wlan profile (continued)	advanced	tx data rate maximum	1 Mbps, 2 Mbps, 5.5 Mbps, 6 Mbps, 9 Mbps, 11 Mbps, 12 Mbps, 18 Mbps, 24 Mbps, 36 Mbps, 48 Mbps, 54 Mbps, mcs0, mcs1, mcs2, mcs3, mcs4, mcs5, mcs6, mcs7	Default: 54 Mbps
		tx data rate	fixed, auto-reduction	Default: auto-reduction
		tx power maximum		Default: 17 dBm
		antenna diversity	enabled, antenna 1, antenna 2	Default: enabled
		power management	enable, disable	Default: disable
		power management interval		Default: 1 beacons (100 msec each)
	security	suite	none, wep, wpa, wpa2	Default: none
		key type	passphrase, hex	Default: passphrase
		passphrase		Value is SECRET, hidden from user view.
		wep authentication	open, shared	Default: open
		wep key size	40, 104	Default: 40
		wep tx key index	1, 2, 3, 4	Default: 1
		wep key 1		Value is SECRET, hidden from user view.
		wep key 2		Value is SECRET, hidden from user view.
		wep key 3		Value is SECRET, hidden from user view.
		wep key 4		Value is SECRET, hidden from user view.
		wpax authentication	psk, 802.1x	Default: psk
		wpax key		Value is SECRET, hidden from user view.
		wpax ieee 802.1x	leap, eap-tls, eap-ttls, peap	Default: eap-ttls
		wpax eap-ttls option	eap-mschapv2, mschapv2, mschap, chap, pap, eap-md5	Default: eap-mschapv2
		wpax peap option	eap-mschapv2, eap-md5	Default: eap-mschapv2
		wpax username		
		wpax password		Value is SECRET, hidden from user view.

Group Name (continued)	Group Item	Value Name	Value Options	Additional Information
wlan profile (continued)	security (continued)	wpax encryption	ccmp, tkip, wep	May contain zero, one, or more of the values, separated by commas. Default: None
		wpax validate certificate	enable, disable	Default: enable
		wpax credentials		
xml import control	restore factory configuration		enable, disable	
	delete http authentication uris		enable, disable	Deletes existing HTTP authentication URIs before importing new ones.
	http authentication uri delete	name		Deletes the specified HTTP authentication URI.
	reboot		enable, disable	Reboots after importing.

XML Status Record Groups and Items

Table 4-8 lists the supported XML Status Record (XSR) groups and items. These groups and items show the status of the device in XML form and can only be exported. The XSR schema differs slightly from the XCR groups and items in that the XSR allows groups within groups.

Note: *The Valid Values column of Table 4-8 indicates the default value.*

Table 4-8 XSR Group and Items

Group Name	Item Name	Value Name	Valid Values
arp	arp entry	ip address	ip address in format nnn.nnn.nnn.nnn
		mac address	mac address in format xx:xx:xx:xx:xx:xx
		type	dynamic or static
		interface	eth0 or wlan0
bridge (Attribute of "instance" is "br0")	enable state		Enabled or Disabled
	active state		Active or Inactive
device	product info	product type	Lantronix
		serial number	12 hex digits
		firmware version	string in version format like 7.2.0.0R15
		uptime	elapsed time in format d days hh:mm:ss
		permanent config	saved or unsaved
		region	possible values: U.S., European Union, Japan and Worldwide
email (Attribute of "instance" is "<decimal>")	success	sent	decimal number
		sent with retries	decimal number
	failed		decimal number
	queued		decimal number
email log (Attribute of "instance" is "<decimal>")	entry	time	timestamp in format d days hh:mm:ss
		log	string
hardware	cpu	type	string
		speed	form of <decimal> megahertz
	memory	Flash size	decimal number of bytes
		ram size	decimal number of bytes

Group Name (continued)	Item Name	Value Name	Valid Values
http	state		enable or disable
	logging	entries	decimal number
		bytes	decimal number
http log	totals	entries	decimal number
		bytes	decimal number
	entry (Attribute of "instance" is "<decimal>")		String
icmp	snmp	InMsgs	decimal number
		InErrors	decimal number
		InDestUnreachs	decimal number
		InTimeExcds	decimal number
		InParmProbs	decimal number
		InSrcQuenchs	decimal number
		InRedirects	decimal number
		InEchos	decimal number
		InEchoReps	decimal number
		InTimestamps	decimal number
		InTimestampReps	decimal number
		InAddrMasks	decimal number
		InAddrMaskReps	decimal number
		OutMsgs	decimal number
		OutErrors	decimal number
		OutDestUnreachs	decimal number
		OutTimeExcds	decimal number
		OutParmProbs	decimal number
		OutSrcQuenchs	decimal number
		OutRedirects	decimal number
		OutEchos	decimal number
		OutEchoReps	decimal number
		OutTimestamps	decimal number
		OutTimestampReps	decimal number
		OutAddrMasks	decimal number
		OutAddrMaskReps	decimal number
interface (Attribute of "instance" is "eth0")	generic	status	linkup
	ip address		dotted notation
	network mask		dotted notation
	default gateway		dotted notation

Group Name (continued)	Item Name	Value Name	Valid Values
interface (Attribute of "instance" is "eth0") (continued)	receive	bytes	decimal number
		packets	decimal number
		errs	decimal number
		drop	decimal number
		fifo	decimal number
		frame	decimal number
		compressed	decimal number
		multicast	decimal number
	transmit	bytes	decimal number
		packets	decimal number
		errs	decimal number
		drop	decimal number
		fifo	decimal number
		colls	decimal number
		carrier	decimal number
		compressed	decimal number
ip	snmp	Forwarding	decimal number
		DefaultTTL	decimal number
		InReceives	decimal number
		InHdrErrors	decimal number
		InAddrErrors	decimal number
		ForwDatagrams	decimal number
		InUnknownProtos	decimal number
		InDiscards	decimal number
		InDelivers	decimal number
		OutRequests	decimal number
		OutDiscards	decimal number
		OutNoRoutes	decimal number
		ReasmTimeout	decimal number
		ReasmReqds	decimal number
		ReasmOKs	decimal number
		ReasmFails	decimal number
		FragOKs	decimal number
		FragFails	decimal number
		FragCreates	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
ip (continued)	netstat	InNoRoutes	decimal number
		InTruncatedPkts	decimal number
		InMcastPkts	decimal number
		OutMcastPkts	decimal number
		InBcastPkts	decimal number
		OutBcastPkts	decimal number
ip sockets	ip socket	protocol	tcp or udp
		rx queue	decimal number
		tx queue	decimal number
		local address	ip address in format nnn.nnn.nnn.nnn
		local port	decimal number
		remote address	ip address in format nnn.nnn.nnn.nnn
		remote port	decimal number or *
		state	LISTEN, SYN_RECVD, SYN_SENT, ESTABLISHED, CLOSE_WAIT, LAST_ACK, FIN_WAIT_1, FIN_WAIT_2, CLOSING, or TIME_WAIT.
line (Attribute of "instance" is "<decimal>")	receiver	bytes	decimal number
		breaks	decimal number
		parity errors	decimal number
		framing errors	decimal number
		overrun errors	decimal number
		no receive buffer errors	decimal number
		queued bytes	decimal number
		flow control	go, stop, or n/a
	transmitter	bytes	decimal number
		breaks	decimal number
		queued bytes	decimal number
		flow control	go, stop, or n/a
	line levels	cts	asserted or not asserted
		rts	asserted or not asserted
		dsr	asserted or not asserted
		dtr	asserted or not asserted

Group Name (continued)	Item Name	Value Name	Valid Values
line (group nested within line above)	state		enable or disable
	protocol		Tunnel or None.
	baud rate		<decimal> bits per second
	parity		None, Odd, or Even
	data bits		7 or 8
	stop bits		1 or 2
	flow control		None, Hardware, or Software
	xon char		of form <control>Q
	xoff char		of form <control>S
memory	main heap	total memory	decimal number of bytes
		available memory	decimal number of bytes
processes	process (Attribute of "instance" is "<decimal>")	stack used	decimal number
		stack size	decimal number
		cpu %	decimal number
		thread name	String
query port	status		enabled or disabled
	last connection	ip address	ip address in format nnn.nnn.nnn.nnn
		port	decimal number
	in	discoveries	decimal number
		unknown queries	decimal number
		erroneous packets	decimal number
	out	discovery replies	decimal number
		errors	decimal number
rss	url		string in the form of a web url
	data	entries	decimal number
		bytes	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
sessions	telnet or ssh (Attribute of "instance" is "<decimal>")	local port	decimal number
		remote ip address	ip address in format nnn.nnn.nnn.nnn
		remote port	decimal number
		duration	elapsed time in format d days hh:mm:ss
	line (Attribute of “instance” is <decimal>)	baud	decimal number
		parity	decimal number
		databits	decimal number
		stop bits	decimal number
		flow control	
tcp	snmp	RtoAlgorithm	decimal number
		RtoMin	decimal number
		RtoMax	decimal number
		MaxConn	decimal number
		ActiveOpens	decimal number
		PassiveOpens	decimal number
		AttemptFails	decimal number
		EstabResets	decimal number
		CurrEstab	decimal number
		InSegs	decimal number
		OutSegs	decimal number
		RetransSegs	decimal number
		InErrs	decimal number
		OutRsts	decimal number
	netstat	SyncookiesSent	decimal number
		SyncookiesRecv	decimal number
		SyncookiesFailed	decimal number
		EmbryonicRsts	decimal number
		PruneCalled	decimal number
		RcvPruned	decimal number
		OfoPruned	decimal number
		OutOfWindowIcmps	decimal number
		LockDroppedIcmps	decimal number
		ArpFilter	decimal number
		TW	decimal number
		TWRecycled	decimal number
		TWKilled	decimal number
		PAWSPassive	decimal number
		PAWSActive	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
tcp (continued)	netstat (continued)	PAWSEstab	decimal number
		DelayedACKs	decimal number
		DelayedACKLocked	decimal number
		DelayedACKLost	decimal number
		ListenOverflows	decimal number
		ListenDrops	decimal number
		TCPPrequeued	decimal number
		TCPDirectCopyFromBacklog	decimal number
		TCPDirectCopyFromPrequeue	decimal number
		TCPPrequeueDropped	decimal number
		TCPHPHits	decimal number
		TCPHPHitsToUser	decimal number
		TCPPureAcks	decimal number
		TCPHPAcks	decimal number
		TCPRenoRecovery	decimal number
		TCPSackRecovery	decimal number
		TCPSACKReneging	decimal number
		TCPFACKReorder	decimal number
		TCPSACKReorder	decimal number
		TCPRenoReorder	decimal number
		TCPTSReorder	decimal number
		TCPFullUndo	decimal number
		TCPPartialUndo	decimal number
		TCPDSACKUndo	decimal number
		TCPLossUndo	decimal number
		TCPLoss	decimal number
		TCPLostRetransmit	decimal number
		TCPRenoFailures	decimal number
		TCPSackFailures	decimal number
		TCPLossFailures	decimal number
		TCPFastRetrans	decimal number
		TCPForwardRetrans	decimal number
		TCPSlowStartRetrans	decimal number
		TCPTimeouts	decimal number
		TCPRenoRecoveryFail	decimal number
		TCPSackRecoveryFail	decimal number
		TCPSchedulerFailed	decimal number
		TCPRcvCollapsed	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
tcp (continued)	netstat (continued)	TCPDSACKOldSent	decimal number
		TCPDSACKOfoSent	decimal number
		TCPDSACKRecv	decimal number
		TCPDSACKOfoRecv	decimal number
		TCPAbortOnSyn	decimal number
		TCPAbortOnData	decimal number
		TCPAbortOnClose	decimal number
		TCPAbortOnMemory	decimal number
		TCPAbortOnTimeout	decimal number
		TCPAbortOnLinger	decimal number
		TCPAbortFailed	decimal number
		TCPMemoryPressures	decimal number
		TCPSACKDiscard	decimal number
		TCPDSACKIgnoredOld	decimal number
		TCPDSACKIgnoredNoUndo	decimal number
		TCPSpuriousRTOs	decimal number
		TCPMD5NotFound	decimal number
		TCPMD5Unexpected	decimal number
		TCPSackShifted	decimal number
		TCPSackMerged	decimal number
		TCPSackShiftFallback	decimal number
tunnel	aggregate	completed connects	decimal number
		completed accepts	decimal number
		disconnects	decimal number
		dropped connects	decimal number
		dropped accepts	decimal number
		octets from serial	decimal number
		octets from network	decimal number
		connect 0 connection time	elapsed time in format d days hh:mm:ss
		connect 1 connection time	elapsed time in format d days hh:mm:ss
		connect 2 connection time	elapsed time in format d days hh:mm:ss
		connect 3 connection time	elapsed time in format d days hh:mm:ss
		connect 4 connection time	elapsed time in format d days hh:mm:ss
		connect 5 connection time	elapsed time in format d days hh:mm:ss

Group Name (continued)	Item Name	Value Name	Valid Values
tunnel (continued)	aggregate (continued)	connect 6 connection time	elapsed time in format d days hh:mm:ss
		connect 7 connection time	elapsed time in format d days hh:mm:ss
		connect 8 connection time	elapsed time in format d days hh:mm:ss
		connect 9 connection time	elapsed time in format d days hh:mm:ss
		connect 10 connection time	elapsed time in format d days hh:mm:ss
		connect 11 connection time	elapsed time in format d days hh:mm:ss
		connect 12 connection time	elapsed time in format d days hh:mm:ss
		connect 13 connection time	elapsed time in format d days hh:mm:ss
		connect 14 connection time	elapsed time in format d days hh:mm:ss
		connect 15 connection time	elapsed time in format d days hh:mm:ss
		accept connection time	elapsed time in format d days hh:mm:ss
		connect dns address changes	decimal number
		connect dns address invalids	decimal number
tunnel modem	echo commands		
	verbose response		
	response type		
	error unknown commands		
	incoming connection		
udp	snmp	InDatagrams	decimal number
		NoPorts	decimal number
		InErrors	decimal number
		OutDatagrams	decimal number
		RcvbufErrors	decimal number
		SndbufErrors	decimal number

Group Name (continued)	Item Name	Value Name	Valid Values
vip	data bytes	receive	decimal number
		transmit	decimal number
	udp packet queue	receive	decimal number
		transmit	decimal number
	udp packets	receive	decimal number
		transmit	decimal number
	dsm ip address list		ip address in format nnn.nnn.nnn.nnn For more than one, comma will separate.
	local dna id		
	tunnel user		
	tunnel port list		Comma separated list of decimal numbers.
	tunnel http port list		Comma separated list of decimal numbers.
	current dsm ip address		ip address in format nnn.nnn.nnn.nnn
	current tunnel port		decimal number
	tunnel proxy host		ip address in format nnn.nnn.nnn.nnn
	tunnel proxy port		decimal number
	conduit status		Disabled, Down, Attempting connection, Idle, Negotiating, Up, or Closing.
	conduit uptime		elapsed time in format d days hh:mm:ss
	time of last replication		timestamp in format d days hh:mm:ss
	config name		
	vip pools		decimal number
wlan status	type		
	bssid		
	ssid		
	topology		
	active wlan profile		
	pairwise cipher		
	group cipher		
	authentication		
	security suite		
	channel		
	ip address		

Group Name (continued)	Item Name	Value Name	Valid Values
wlan status (continued)	rssi		
	wps mode		
wlan scan*	network name	bssid	
		channel	
		rssi	
		topology	
xsr	out	bytes	decimal number
		lines	decimal number
		elements	decimal number
	errors		decimal number

Note: **If a scan is run while the unit is associated with an access point, only the channels belonging to the band on which the device is currently operating will be scanned.*

5: Commands and Levels

Click the level in the tree structure and it will take you to the command list for that level.

root

- enable (enable)
  - configure (config)
    - arp (config-arp)
    - bridge 1 (config-bridge:br0)
    - cli (config-cli)
      - ssh (config-cli-ssh)
      - telnet (config-cli-telnet)
    - diagnostics (config-diagnostics)
      - log (config-diagnostics-log)
    - ftp (config-ftp)
    - host 1 (config-host:1)
    - host 2 (config-host:2)
    - host 3 (config-host:3)
    - host 4 (config-host:4)
    - host 5 (config-host:5)
    - host 6 (config-host:6)
    - host 7 (config-host:7)
    - host 8 (config-host:8)
    - host 9 (config-host:9)
    - host 10 (config-host:10)
    - host 11 (config-host:11)
    - host 12 (config-host:12)
    - host 13 (config-host:13)
    - host 14 (config-host:14)
    - host 15 (config-host:15)
    - host 16 (config-host:16)
    - host 17 (config-host:17)
    - host 18 (config-host:18)
    - host 19 (config-host:19)
    - host 20 (config-host:20)
    - host 21 (config-host:21)
    - host 22 (config-host:22)
    - host 23 (config-host:23)
    - host 24 (config-host:24)
    - host 25 (config-host:25)
    - host 26 (config-host:26)
    - host 27 (config-host:27)
    - host 28 (config-host:28)
    - host 29 (config-host:29)
    - host 30 (config-host:30)
    - host 31 (config-host:31)
    - host 32 (config-host:32)
    - http (config-http)
    - icmp (config-icmp)
    - if 1 (config-if:eth0)
      - link (config-ethernet:eth0)
    - if 2 (config-if:wlan0)

- link (config-wlan:wlan0)
  - choice 1 (config-wlan-choice:wlan0:1)
  - choice 2 (config-wlan-choice:wlan0:2)
  - choice 3 (config-wlan-choice:wlan0:3)
  - choice 4 (config-wlan-choice:wlan0:4)
- ip (config-ip)
- query port (config-query_port)
- rss (config-rss)
- smtp (config-smtp)
- syslog (config-syslog)
- terminal 1 (config-terminal:1)
- terminal 2 (config-terminal:2)
- terminal network (config-terminal:network)
- vip (config-vip)
- wlan profiles (config-profiles)

- device (device)
- dns (dns)
- email 1 (email:1)
- email 2 (email:2)
- email 3 (email:3)
- email 4 (email:4)
- email 5 (email:5)
- email 6 (email:6)
- email 7 (email:7)
- email 8 (email:8)
- email 9 (email:9)
- email 10 (email:10)
- email 11 (email:11)
- email 12 (email:12)
- email 13 (email:13)
- email 14 (email:14)
- email 15 (email:15)
- email 16 (email:16)
- filesystem (filesystem)
- line 1 (line:1)
- line 2 (line:2)
- ssh (ssh)
  - client (ssh-client)
  - server (ssh-server)
- ssl (ssl)
  - credentials (ssl-credentials)
  - trusted authorities (ssl-auth)
- tunnel 1 (tunnel:1)
  - accept (tunnel-accept:1)
    - password (tunnel-accept-password:1)
  - connect (tunnel-connect:1)
    - host 1 (tunnel-connect-host:1:1)
    - host 2 (tunnel-connect-host:1:2)
    - host 3 (tunnel-connect-host:1:3)
    - host 4 (tunnel-connect-host:1:4)
    - host 5 (tunnel-connect-host:1:5)
    - host 6 (tunnel-connect-host:1:6)
    - host 7 (tunnel-connect-host:1:7)

- host 8 (tunnel-connect-host:1:8)
- host 9 (tunnel-connect-host:1:9)
- host 10 (tunnel-connect-host:1:10)
- host 11 (tunnel-connect-host:1:11)
- host 12 (tunnel-connect-host:1:12)
- host 13 (tunnel-connect-host:1:13)
- host 14 (tunnel-connect-host:1:14)
- host 15 (tunnel-connect-host:1:15)
- host 16 (tunnel-connect-host:1:16)

- disconnect (tunnel-disconnect:1)
- modem (tunnel-modem:1)
- packing (tunnel-packing:1)
- serial (tunnel-serial:1)

- tunnel 2 (tunnel:2)
  - accept (tunnel-accept:2)
    - password (tunnel-accept-password:2)
  - connect (tunnel-connect:2)
    - host 1 (tunnel-connect-host:2:1)
    - host 2 (tunnel-connect-host:2:2)
    - host 3 (tunnel-connect-host:2:3)
    - host 4 (tunnel-connect-host:2:4)
    - host 5 (tunnel-connect-host:2:5)
    - host 6 (tunnel-connect-host:2:6)
    - host 7 (tunnel-connect-host:2:7)
    - host 8 (tunnel-connect-host:2:8)
    - host 9 (tunnel-connect-host:2:9)
    - host 10 (tunnel-connect-host:2:10)
    - host 11 (tunnel-connect-host:2:11)
    - host 12 (tunnel-connect-host:2:12)
    - host 13 (tunnel-connect-host:2:13)
    - host 14 (tunnel-connect-host:2:14)
    - host 15 (tunnel-connect-host:2:15)
    - host 16 (tunnel-connect-host:2:16)
  - disconnect (tunnel-disconnect:2)
  - modem (tunnel-modem:2)
  - packing (tunnel-packing:2)
  - serial (tunnel-serial:2)
- xml (xml)

Table 5-1 Commands and Levels

accept (tunnel-accept:2) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <*hexadecimal*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".

default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
kill connection	Disconnects the active accept mode tunneling connection.
local port <*number*>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no tcp keep alive	Disables the accept mode TCP keep alive timeout.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel accept status.
start character <*control*>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C.

	A decimal value character has the form \99. A hex value character has the form 0xFF.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
write	Stores the current configuration in permanent memory.
accept (tunnel-accept:1) level commands	
accept mode always	Enables the tunneling server to always accept tunneling connections.
accept mode any character	Enables the tunneling server to accept tunneling connections only when a character is received through the corresponding line (serial port).
accept mode disable	Disables accept mode tunneling.
accept mode modem control asserted	Enables the tunneling server to accept tunneling connections when the modem control pin is asserted.
accept mode modem emulation	Enables modem emulation for accept mode tunneling.
accept mode start character	Enables accept mode tunneling when the configured start character is received on the line.
aes decrypt key <*hexadecimal*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the accept tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the accept tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
block network disable	Forwards (tunnels) network data in accept mode tunneling.
block network enable	Discards all data coming in from the accept mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in accept mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the accept mode tunnel (generally used for debugging).

clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL server.
default accept mode	Restores the default accept mode as "always".
default local port	Uses the default port number as the local port for accept mode tunneling. The default port is 10000 + #, where # is the line number for this tunnel.
default protocol	Restores the default protocol as "TCP".
default start character	Defaults the accept mode start character.
default tcp keep alive	Restores the default 45 second accept mode TCP keep alive timeout.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing an accept mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing an accept mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing an accept mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing an accept mode tunneling connection.
flush start character disable	Enables forwarding of the accept start character into the network.
flush start character enable	Disables forwarding of the accept start character into the network.
kill connection	Disconnects the active accept mode tunneling connection.
local port <*number*>	Sets the port to use for accept mode tunneling. <number> = number of the port to use.
no aes decrypt key	Removes the accept tunnel AES decrypt key.
no aes encrypt key	Removes the accept tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no email connect	Discontinues sending email alerts upon establishing an accept mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing an accept mode tunnel.
no tcp keep alive	Disables the accept mode TCP keep alive timeout.
password	Enters the next lower level.
protocol ssh	Uses SSH protocol for accept mode tunneling.
protocol ssl	Uses SSL protocol for accept mode tunneling.
protocol tcp	Uses TCP protocol for accept mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for accept mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for accept mode tunneling.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show status	Displays tunnel accept status.
start character <*control*>	Sets the accept mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for accept mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
write	Stores the current configuration in permanent memory.
arp (config-arp) level commands	
add <*IP address*> <*MAC address*>	Adds an entry to the ARP table, mapping an IP address to a MAC address. <ip address> = IP address to be mapped. <mac address> = MAC address in colon-separated form.
clrscrn	Clears the screen.
exit	Exits to the configuration level.
remove all	Removes all entries from the ARP cache.
remove ip <*IP address*>	Removes an entry from the ARP cache. <ip address> = address of the entry being removed.
show cache	Displays the ARP cache table.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
bridge 1 (config-bridge:br0) level commands	
bridging mac address <*hexadecimal*>	Sets the Bridging MAC Address. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
clrscrn	Clears the screen.
exit	Exits to the config level.
no bridging mac address	Removes the Bridging MAC Address.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Show bridge statistics
show status	Show bridge status
state disable	Disables bridging.
state enable	Enables bridging.
write	Stores the current configuration in permanent memory.
choice 1 (config-wlan-choice:wlan0:1) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile <*text*>	Selects a profile. <text> = name of the profile.

show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
choice 2 (config-wlan-choice:wlan0:2) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile <*text*>	Selects a profile. <text> = name of the profile.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
choice 3 (config-wlan-choice:wlan0:3) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile <*text*>	Selects a profile. <text> = name of the profile.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
choice 4 (config-wlan-choice:wlan0:4) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no profile	Removes reference to the profile.
profile <*text*>	Selects a profile. <text> = name of the profile.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
cli (config-cli) level commands	
clrscrn	Clears the screen.
default inactivity timeout	The default inactivity timeout will apply to CLI sessions.
default login password	Restores the default CLI login password.
default quit connect line	Restores the default string used to quit the "connect line <line>" command.
enable level password <*text*>	Sets the enable-level password.
exit	Exits to the configuration level.

inactivity timeout <*minutes*>	Sets the inactivity timeout for all CLI sessions.
line authentication disable	No password required for Line CLI users.
line authentication enable	Challenges the Line CLI user with a password.
login password <*text*>	Sets the CLI login password.
no enable level password	Removes the enable-level password.
no inactivity timeout	No inactivity timeout will apply to CLI sessions.
quit connect line <*control*>	Sets the string used to quit the "connect line <line>" command. The characters may be input as text or control. A control character has the form <control>C.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh	Change to menu level for SSH configuration and status.
telnet	Change to menu level for Telnet configuration and status.
write	Stores the current configuration in permanent memory.
client (ssh-client) level commands	
clrscrn	Clears the screen.
default user <*username*> command	Restore the user command to the default login shell
delete all known hosts	Remove all hnown hosts
delete all users	Remove all users
delete known host <*server*>	Remove known host
delete user <*username*>	Delete the named user
exit	Exits to the ssh level.
known host <*server*>	Set known host RSA or DSA key
no known host <*server*> dsa	Remove known host DSA key
no known host <*server*> rsa	Remove known host RSA key
no user <*username*> dsa	Remove user DSA key
no user <*username*> rsa	Remove user RSA key
show	Show SSH Client settings
show history	Displays the last 20 commands entered during the current CLI session.
show known host <*server*>	Show known host RSA and DSA keys
show user <*username*>	Show information for a user
user <*username*>	Set username and RSA or DSA keys
user <*username*> command <*command*>	Customizes the user command
user <*username*> generate dsa 1024	Generate DSA public and private keys
user <*username*> generate dsa 512	Generate DSA public and private keys
user <*username*> generate dsa 768	Generate DSA public and private keys
user <*username*> generate rsa 1024	Generate RSA public and private keys
user <*username*> generate rsa 512	Generate RSA public and private keys
user <*username*> generate rsa 768	Generate RSA public and private keys
user <*username*> password <*password*>	Set username with password and optional RSA or DSA keys
write	Stores the current configuration in permanent memory.
configure (config) level commands	
arp	Changes to the command level for ARP configuration and status.
bridge <*instance*>	Changes to the bridge configuration level.
cli	Change to menu level for CLI configuration and status

clrscrn	Clears the screen.
diagnostics	Enters the diagnostics level.
exit	Exits to the enable level.
ftp	Enters the ftp level.
host <*number*>	Change to config host level
http	Enters the http level.
icmp	Changes to the command level for ICMP configuration and status.
if <*instance*>	Changes to the interface configuration level.
ip	Changes to the command level for IP configuration and status.
kill ssh <*session*>	Kills SSH session with index from "show sessions"
kill telnet <*session*>	Kills Telnet session with index from "show sessions"
query port	Enters the query port level.
rss	Change to menu level for RSS configuration and status
show	Displays system information.
show history	Displays the last 20 commands entered during the current CLI session.
smtp	Changes to the command level for SMTP configuration and status.
syslog	Enters the syslog level.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
vip	Change to menu level for VIP configuration and status
wlan profiles	Enters the WLAN profiles configuration level.
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:2) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured

	start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <*instance*>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <*number*>	Sets a specific port for use as the local port. <number> = the number of the port to use.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <*number*>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <*milliseconds*>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.

start character <*control*>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
connect (tunnel-connect:1) level commands	
block network disable	Forwards (tunnels) network data in connect mode tunneling.
block network enable	Discards all data coming in from the connect mode tunnel before forwarding it to the serial interface (generally used for debugging).
block serial disable	Forwards (tunnels) serial data in connect mode tunneling.
block serial enable	Discards all data coming in from the serial interface before forwarding it to the connect mode tunnel (generally used for debugging).
clrscrn	Clears the screen.
connect mode always	Enables the tunneling server to always establish tunneling connections.
connect mode any character	Enables the tunneling server to establish a tunneling connection when a character is received on the corresponding line (serial port).
connect mode disable	Disables connect mode tunneling.
connect mode modem control asserted	Enables the tunneling server to make tunneling connections when the modem control pin is asserted.
connect mode modem emulation	Enables modem emulation for connect mode tunneling.
connect mode start character	Enables connect mode tunneling when the configured start character is received on the line.
default connect mode	Restores the default connect mode as "disable".
default host mode	Connects to the first host in the list that accepts the connection.
default local port	Uses a random port number as the local port for establishing tunneling connections to other devices.
default reconnect time	Restores the default reconnect time value for connect mode tunneling.
default start character	Defaults the connect mode start character.
email connect <*number*>	Sets an email profile to use to send an email alert upon establishing a connect mode tunnel. <number> = the number of the email profile to use.
email disconnect <*number*>	Sets an email profile to use to send an email alert upon closing a connect mode tunnel. <number> = the number of the email profile to use.
exit	Returns to the tunnel level.
flush serial disable	Characters already in the serial data buffer are retained upon establishing a connect mode tunneling connection.
flush serial enable	Flushes the serial data buffer upon establishing a connect

	mode tunneling connection.
flush start character disable	Enables forwarding of the connect start character into the network.
flush start character enable	Disables forwarding of the connect start character into the network.
host <*instance*>	Enters the next lower level. Specify the instance for the next lower level.
host mode sequential	Connects to the first host in the list that accepts the connection.
host mode simultaneous	Selects simultaneous connections to all hosts on the host list.
kill connection	Disconnects the active connect mode tunneling connection or connections.
local port <*number*>	Sets a specific port for use as the local port. <number> = the number of the port to use.
no email connect	Discontinues sending email alerts upon establishing a connect mode tunnel.
no email disconnect	Discontinues sending email alerts upon closing a connect mode tunnel.
promote host <*number*>	Promotes the identified host, exchanging it place with the host above it, to adjust the order of the defined hosts.
reconnect time <*milliseconds*>	Sets the reconnect time value for tunneling connections established by the device in milliseconds. <milliseconds> = timeout in milliseconds.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel connect status.
start character <*control*>	Sets the connect mode start character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
credentials (ssl-credentials) level commands	
clrscrn	Clears the screen.
create <*credential name*>	Create a new credential name
delete <*credential name*>	Delete existing credential by name
edit <*credential name*>	View or edit an existing profile
exit	Exits to the ssl level.
show	Show existing credential names
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
device (device) level commands	
auto show tlog	Continuously displays the internal trouble log.
clrscrn	Clears the screen.
exit	Exit to the enable level.
show	Show system information

show hardware information	Displays information about the hardware.
show history	Displays the last 20 commands entered during the current CLI session.
show memory	Displays current memory usage information.
show task state	Displays current task states.
show tlog	Displays the internal trouble log.
write	Stores the current configuration in permanent memory.
diagnostics (config-diagnostics) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
log	Enters the next lower level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:2) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.
flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character *<control>*	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
timeout *<milliseconds>*	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.
write	Stores the current configuration in permanent memory.
disconnect (tunnel-disconnect:1) level commands	
clrscrn	Clears the screen.
exit	Returns to the tunnel level.
flush serial disable	Does not flush serial data upon closing a tunneling connection.
flush serial enable	Flushes serial data buffer when a tunneling connection is closed.

flush stop character disable	Forwards the stop character from the Line to the network.
flush stop character enable	Prevents the stop character from the Line from being forwarded to the network.
modem control disable	Does not watch the modem control pin to disconnect.
modem control enable	Watches the modem control pin and disconnects if it is not asserted.
no stop character	Removes the stop character.
no timeout	Disables disconnect after timeout feature for tunneling sessions.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
stop character *<control>*	Sets the stop character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
timeout *<milliseconds>*	Disconnects when no data has been received on the line (serial port) for the specified length of time. <milliseconds> = timeout in milliseconds.
write	Stores the current configuration in permanent memory.
dns (dns) level commands	
clrscrn	Clears the screen.
exit	Exits to the enable level.
lookup *<host_or_ip>*	Return a lookup on the DNS name or IP address.
show	Show DNS status.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
email 1 (email:1) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert.

	<text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 10 (email:10) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.

from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 11 (email:11) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.

clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <*number*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*text*>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain <*text*>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <*text*>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port <*number*>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <*text*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.

email 12 (email:12) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 13 (email:13) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts.

	<text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port <*number*>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <*text*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 14 (email:14) level commands	
auto show statistics	Continuously displays email statistics.
cc <*text*>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <*number*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*text*>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain <*text*>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain

	name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 15 (email:15) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.

no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 16 (email:16) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert.

	<text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 2 (email:2) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.

from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 3 (email:3) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.

clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <*number*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*text*>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain <*text*>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to <*text*>	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port <*number*>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <*text*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.

email 4 (email:4) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.

show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 5 (email:5) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts.

	<text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port <*number*>	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject <*text*>	Sets the Subject for email alerts. <text> = text to placed as the subject.
to <*text*>	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 6 (email:6) level commands	
auto show statistics	Continuously displays email statistics.
cc <*text*>	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email <*number*>	Enters the configure email level.
exit	Exits to the enable level.
from <*text*>	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port <*number*>	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file <*text*>	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain <*text*>	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain

	name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 7 (email:7) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.

no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 8 (email:8) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.
from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert.

	<text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
email 9 (email:9) level commands	
auto show statistics	Continuously displays email statistics.
cc *<text>*	Sets Cc addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
clear log	Clears all entries from the mail log.
clear mail counters	Sets the email counters to zero.
clrscrn	Clears the screen.
default local port	Sets the local port (used to send email alerts) to random.
default priority	Sets X-Priority for email alerts to 3 (normal).
default server port	Restores the factory default port for SMTP on the server side.
email *<number>*	Enters the configure email level.
exit	Exits to the enable level.

from *<text>*	Sets the From address for email alerts. <text> = email address to place in the From field of the email alert.
local port *<number>*	Sets the local port used to send email alerts. <number> local port to use for email alerts.
message file *<text>*	Specifies a text file, the contents of which will be the message body of an email alert. <text> = the name of a local file.
no cc	Removes the Cc addresses for email alerts.
no clear mail counters	Restores the email counters to the aggregate values.
no from	Removes the From address for email alerts.
no message file	Removes the file name, so the message body will be empty.
no overriding domain	Removes the overriding domain name option.
no reply to	Removes the Reply To address for email alerts.
no subject	Removes subject used for email alerts.
no to	Removes the To addresses for email alerts.
overriding domain *<text>*	Sets a domain name that will be used when connecting to an SMTP server to send an email alert instead of the device's domain name in EHLO. <text> = domain name to override the current domain name in EHLO.
priority high	Sets X-Priority for email alerts to 2 (high).
priority low	Sets X-Priority for email alerts to 4 (low).
priority normal	Sets X-Priority for email alerts to 3 (normal).
priority urgent	Sets X-Priority for email alerts to 1 (urgent).
priority very low	Sets X-Priority for email alerts to 5 (very low).
reply to *<text>*	Sets the Reply To address for email alerts. <text> = email address to place in the Reply To field of the email alert.
send	Sends an email using the current settings.
server port *<number>*	Sets the port used by the SMTP server. <number> = port used for SMTP on the server side.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the email log.
show statistics	Displays email statistics.
subject *<text>*	Sets the Subject for email alerts. <text> = text to placed as the subject.
to *<text>*	Sets To addresses for email alerts. <text> = a quoted, semicolon separated list of email addresses.
write	Stores the current configuration in permanent memory.
enable (enable) level commands	
auto show interfaces	Show interface statistics
auto show processes	Continuously show thread runtime information
clrscrn	Clears the screen.
configure	Enters the configuration level.
connect	Show name and number for lines.

connect line <*line*>	Begin session on serial port.
device	Enters the device level.
disable	Exits the enable level.
dns	Enters the DNS level.
email <*number*>	Enters the configure email level.
exit	Exit from the system
filesystem	Enters the filesystem level.
kill ssh <*session*>	Kills SSH session with index from "show sessions"
kill telnet <*session*>	Kills Telnet session with index from "show sessions"
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
ping <*host*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	Ping destination n times with x timeout (in seconds)
reload	Reboot system
reload factory defaults	Reload factory defaults to permanent storage
show	Show system information
show history	Displays the last 20 commands entered during the current CLI session.
show interfaces	Show interface statistics
show ip sockets	Show UDP/TCP state information
show processes	Show thread runtime information
show sessions	Show active Telnet and SSH Sessions
ssh	Enters the SSH configuration level.
ssh <*optClientUsername*> <*host*>	Begin SSH session on network <host>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.
ssh <*optClientUsername*> <*host*> <*port*>	Begin SSH session on network <host>:<port>. The optClientUserName must match an SSH Client: Users configuration entry. Use "" in optClientUserName to prompt for host username and password.
ssl	Enters the SSL configuration level.
telnet <*host*>	Begin telnet session on network <host>.
telnet <*host*> <*port*>	Begin telnet session on network <host>:<port>.
trace route <*host*>	Trace route to destination
trace route <*host*> <*protocol*>	Trace route to destination using TCP, ICMP, or UDP
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xml	Enters the XML level.
filesystem (filesystem) level commands	
cat <*file*>	Show the contents of a file
cd <*directory*>	Change the current directory to the specified directory
clrscrn	Clears the screen.
cp <*source file*> <*destination file*>	Copy an existing file
dump <*file*>	Show contents of a file as a hex dump
exit	Exits to the enable level.

format	Format the file system and lose all data
ls	Show all files and directories in the current directory
ls <*directory*>	Show all files and directories in the specified directory
mkdir <*directory*>	Create a directory
mv <*source file*> <*destination file*>	Move a file on the file system
pwd	Print working directory
rm <*file*>	Remove a file
rmdir <*directory*>	Remove a directory
show	Show file system statistics
show history	Displays the last 20 commands entered during the current CLI session.
show tree	Show all files and directories from current directory
tftp get <*source file*> <*destination file*> <*host*>	Get a file using TFTP
tftp get <*source file*> <*destination file*> <*host*> <*port*>	Get a file using TFTP
tftp put <*source file*> <*destination file*> <*host*>	Put a file using TFTP
tftp put <*source file*> <*destination file*> <*host*> <*port*>	Put a file using TFTP
touch <*file*>	Create a file
ftp (config-ftp) level commands	
clrscrn	Clears the screen.
exit	Returns to the config level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the FTP statistics.
state disable	Disables the FTP server.
state enable	Enables the FTP server.
write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:2:1) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16

	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.

write	Stores the current configuration in permanent memory.
host 1 (tunnel-connect-host:1:1) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode

	tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username *<text>*	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive *<milliseconds>*	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name *<text>*	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 1 (config-host:1) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host *<number>*	Change to config host level
name *<text>*	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address *<text>*	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.

host 10 (tunnel-connect-host:2:10) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.

protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (tunnel-connect-host:1:10) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.

credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 10 (config-host:10) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value,

	which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:2:11) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL

	client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (tunnel-connect-host:1:11) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes.

	Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.

show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 11 (config-host:11) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:2:12) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits.

	Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (tunnel-connect-host:1:12) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 12 (config-host:12) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.

no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:2:13) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc-tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc-tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.

no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (tunnel-connect-host:1:13) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character.

	Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and

	sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 13 (config-host:13) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:2:14) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.

validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (tunnel-connect-host:1:14) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.

no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 14 (config-host:14) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host.

	<number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:2:15) level commands	
address *<text>*	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key *<hexadecimal>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text *<text>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key *<hexadecimal>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text *<text>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials *<text>*	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.

port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (tunnel-connect-host:1:15) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains

	spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.

vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 15 (config-host:15) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:2:16) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16

	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.

write	Stores the current configuration in permanent memory.
host 16 (tunnel-connect-host:1:16) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode

	tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username *<text>*	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive *<milliseconds>*	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name *<text>*	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 16 (config-host:16) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host *<number>*	Change to config host level
name *<text>*	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address *<text>*	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.

host 17 (config-host:17) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 18 (config-host:18) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH.

	<text> = username.
write	Stores the current configuration in permanent memory.
host 19 (config-host:19) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:2:2) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16

	bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.

write	Stores the current configuration in permanent memory.
host 2 (tunnel-connect-host:1:2) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode

	tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username *<text>*	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive *<milliseconds>*	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name *<text>*	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 2 (config-host:2) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host *<number>*	Change to config host level
name *<text>*	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address *<text>*	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.

host 20 (config-host:20) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 21 (config-host:21) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH.

	<text> = username.
write	Stores the current configuration in permanent memory.
host 22 (config-host:22) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 23 (config-host:23) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 24 (config-host:24) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host *<number>*	Change to config host level
name *<text>*	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address *<text>*	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 25 (config-host:25) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host *<number>*	Change to config host level
name *<text>*	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address *<text>*	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.

show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 26 (config-host:26) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 27 (config-host:27) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.

remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 28 (config-host:28) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 29 (config-host:29) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is

	selected on the login connect menu. <text> = IP address.
remote port *<number>*	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:2:3) level commands	
address *<text>*	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key *<hexadecimal>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text *<text>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key *<hexadecimal>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text *<text>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials *<text>*	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.

no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (tunnel-connect-host:1:3) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits.

	Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 3 (config-host:3) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 30 (config-host:30) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.

remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 31 (config-host:31) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 32 (config-host:32) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is

	selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:2:4) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.

no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (tunnel-connect-host:1:4) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits.

	Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.

validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 4 (config-host:4) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:2:5) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punc-

	tuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when con-

	necting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (tunnel-connect-host:1:5) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.

protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 5 (config-host:5) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current

	CLI session.
ssh username *<text>*	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:2:6) level commands	
address *<text>*	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key *<hexadecimal>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text *<text>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key *<hexadecimal>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text *<text>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials *<text>*	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port *<number>*	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.

protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (tunnel-connect-host:1:6) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character.

	Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 6 (config-host:6) level commands	

clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:2:7) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.

auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (tunnel-connect-host:1:7) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with.

	<text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.

protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 7 (config-host:7) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:2:8) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16

	bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.

show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username *<text>*	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive *<milliseconds>*	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name *<text>*	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (tunnel-connect-host:1:8) level commands	
address *<text>*	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key *<hexadecimal>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text *<text>*	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key *<hexadecimal>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text *<text>*	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials *<text>*	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.

exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 8 (config-host:8) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.

no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:2:9) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.

no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (tunnel-connect-host:1:9) level commands	
address <*text*>	Sets the remote host to establish tunneling connections with. <text> = IP address or host name of the remote host.
aes decrypt key <*hexadecimal*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.

aes decrypt key text <*text*>	Sets the connect tunnel AES decrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
aes encrypt key <*hexadecimal*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by two adjacent hex digits. Bytes may run together or be separated by optional punctuation: 123ABC "12 3A BC" 12,3A,BC 12.3a.bc 12:3a:bc Note that quotes must enclose the value if it contains spaces.
aes encrypt key text <*text*>	Sets the connect tunnel AES encrypt key with up to 16 bytes. Each byte is represented by a single character. Note that quotes must enclose the value if it contains spaces.
auto show statistics	show connection statistics
clrscrn	Clears the screen.
credentials <*text*>	Selects the RSA/DSA certificates by name for the SSL client.
default protocol	Restores the default protocol as "TCP".
default tcp keep alive	Restores the default 45 second connect mode TCP keep alive timeout.
exit	Exits to the next higher level.
no address	Removes the remote host address used to establish tunneling connections.
no aes decrypt key	Removes the connect tunnel AES decrypt key.
no aes encrypt key	Removes the connect tunnel AES encrypt key.
no credentials	Clears the RSA/DSA certificate selection.
no port	Removes the remote port used to establish tunnel connections.
no ssh username	Removes the SSH user name.
no tcp keep alive	Disables the connect mode TCP keep alive timeout.
no vip name	Removes the VIP name.
port <*number*>	Sets the remote port to use for connect mode tunneling. <number> = number of the port to use.
protocol ssh	Uses SSH protocol for connect mode tunneling.
protocol ssl	Uses SSL protocol for connect mode tunneling.
protocol tcp	Uses TCP protocol for connect mode tunneling.
protocol tcp aes	Uses TCP protocol with AES encryption for connect mode tunneling.
protocol telnet	Uses Telnet protocol (with IAC) for connect mode tunneling.
protocol udp	Uses UDP protocol for connect mode tunneling.
protocol udp aes	Uses UDP protocol with AES encryption for connect mode tunneling.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
ssh username <*text*>	Sets the SSH user name for use when establishing tunneling connections

	with other devices. <text> = SSH user name.
tcp keep alive <*milliseconds*>	Enables TCP keep alive for connect mode tunneling and sets the timer. <milliseconds> = timer value, in milliseconds.
validate certificate disable	Skips verification of the server certificate when connecting.
validate certificate enable	Requires verification of the server certificate when connecting.
vip disable	Makes connections using the specified Address.
vip enable	Makes connections using the VIP name.
vip name <*text*>	Sets the VIP name.
write	Stores the current configuration in permanent memory.
host 9 (config-host:9) level commands	
clrscrn	Clears the screen.
default protocol	Restores the default value of the protocol (Telnet).
default remote port	Sets the remote port (used to connect to the host) to the default value, which depends on the selected protocol.
exit	Exits to the configuration level.
host <*number*>	Change to config host level
name <*text*>	Sets the name of the host. <text> = name of the host.
no name	Clears the name of the host.
no remote address	Clears the remote address of the host.
no ssh username	Clears the SSH username associated with the host.
protocol ssh	Sets the protocol to SSH.
protocol telnet	Sets the protocol to Telnet.
remote address <*text*>	Sets the IP address of the remote host to connect to when this host is selected on the login connect menu. <text> = IP address.
remote port <*number*>	Sets the remote port used to connect to the host. <number> = port to be used.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
ssh username <*text*>	Sets the username for logging into the host via SSH. <text> = username.
write	Stores the current configuration in permanent memory.
http (config-http) level commands	
auth <*uri*>	Creates a new HTTP server authentication directive. <uri> = URI of the server.
auth type <*uri*> digest	Sets an HTTP server authentication directive to the Digest Access Authentication scheme. <uri> = URI of the server.
auth type <*uri*> none	Sets the authentication type for an HTTP server authentication directive to none. <uri> = URI of the server.
auth type <*uri*> ssl	Sets the authentication type for an HTTP server authentication directive to SSL.

	<uri> = URI of the server.
auth type <*uri*> ssl-basic	Sets the authentication type for an HTTP server authentication directive to SSL-Basic. <uri> = URI of the server.
auth type <*uri*> ssl-digest	Sets the authentication type for an HTTP server authentication directive to SSL-Digest. <uri> = URI of the server.
authentication timeout <*minutes*>	For any Digest AuthType, sets the timeout for authentication. <minutes> = authentication timeout value.
clear counters	Sets the HTTP counters to zero.
clear log	Clears the HTTP server log.
clrscrn	Clears the screen.
default authentication timeout	Resets the authentication timeout to its default value.
default log format	Restores the HTTP Server log format string to its default value.
default max bytes	Resets the maximum bytes to its default value.
default max log entries	Restores the default maximum number of HTTP Server log entries.
default max timeout	Resets the timeout to its default value.
default port	Resets the HTTP Server port to its default value.
default secure port	Resets the HTTP Server SSL port to its default value.
default secure protocols	Restores the default secure protocol selections.
delete auth <*uri*>	Deletes an existing HTTP Server authentication directive. <uri> = URI of the server.
exit	Returns to the config level.
log format <*text*>	Sets the log format string for the HTTP server, using the following directives: %a remote ip address (could be a proxy) %b bytes sent excluding headers %B bytes sent excluding headers (0 = '-') %h remote host (same as %a) %{h}i header contents from request (h = header string) %m request method %p ephemeral local port value used for request %q query string (prepend with '?' or empty '-') %t timestamp HH:MM:SS (same as Apache '%(%H:%M:%S)t') %u remote user (could be bogus for 401 status) %U URL path info %r first line of request (same as '%m %U%q <version>') %s return status
logging state disable	Disables HTTP server logging.
logging state enable	Enables HTTP server logging.
max bytes <*number*>	Sets the maximum number of bytes the HTTP server accepts when receiving a request.
max log entries <*number*>	Sets the maximum number of HTTP server log entries. <number> = maximum number of HTTP server log entries.
max timeout <*seconds*>	Sets the maximum time the HTTP server waits when receiving a request. <seconds> = maximum timeout value.

no clear counters	Restores the HTTP counters to the aggregate values.
no port	Disables the HTTP Server port.
no secure credentials	Clears the RSA/DSA certificate selection.
no secure port	Disables the HTTP Server SSL port.
port <*number*>	Sets the port number the HTTP server will use. <number> = port number.
secure credentials <*text*>	Selects the RSA/DSA certificates by name for the HTTP server.
secure port <*number*>	Sets the port number the HTTP server will use over SSL. <number> = port number.
secure protocols ssl3 disable	Disables the protocol.
secure protocols ssl3 enable	Enables the protocol.
secure protocols tls1.0 disable	Disables the protocol.
secure protocols tls1.0 enable	Enables the protocol.
secure protocols tls1.1 disable	Disables the protocol.
secure protocols tls1.1 enable	Enables the protocol.
show	Displays the current configuration.
show auth	Displays the HTTP server authentication settings.
show history	Displays the last 20 commands entered during the current CLI session.
show log	Displays the HTTP server log.
show statistics	Displays the HTTP statistics.
state disable	Disables the HTTP server.
state enable	Enables the HTTP server.
write	Stores the current configuration in permanent memory.
icmp (config-icmp) level commands	
clrscrn	Clears the screen.
exit	Exits to the configuration level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Prevents ICMP packets from being sent or received.
state enable	Allows ICMP packets to be sent and received.
write	Stores the current configuration in permanent memory.
if 1 (config-if:eth0) level commands	
bootp disable	Disables BOOTP.
bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway <*IP address*>	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
dhcp client id <*text*>	Sets the DHCP client id.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
domain <*text*>	Sets the domain name. <text> = name of the domain.
exit	Exits to the config level.
hostname <*text*>	Sets the host name. <text> = name of the host.

if <*instance*>	Changes to the interface configuration level.
ip address <*ip address/cidr*>	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu <*bytes*>	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.
no hostname	Clears the host name.
no ip address	Clears the IP address.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <*IP address*>	Sets the IP address of the primary DNS server.
secondary dns <*IP address*>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
state disable	Disables the interface.
state enable	Enables the interface.
write	Stores the current configuration in permanent memory.
if 2 (config-if:wlan0) level commands	
bootp disable	Disables BOOTP.
bootp enable	Enables BOOTP.
clrscrn	Clears the screen.
default gateway <*IP address*>	Sets the configurable gateway IP address to the default value.
default mtu	Restores the default Maximum Transmission Unit (MTU) size.
dhcp client id <*text*>	Sets the DHCP client id.
dhcp disable	Disables DHCP.
dhcp enable	Enables DHCP.
domain <*text*>	Sets the domain name. <text> = name of the domain.
exit	Exits to the config level.
hostname <*text*>	Sets the host name. <text> = name of the host.
if <*instance*>	Changes to the interface configuration level.
ip address <*ip address/cidr*>	Sets the IP address and network mask. Formats accepted: 192.168.1.1 (default mask) 192.168.1.1/24 (CIDR) "192.168.1.1 255.255.255.0" (explicit mask)
link	Enter link configuration level
mtu <*bytes*>	Sets the Maximum Transmission Unit (MTU) size.
no default gateway	Clears the default gateway.
no dhcp client id	Clears the DHCP client ID.
no domain	Clears the domain name.

no hostname	Clears the host name.
no ip address	Clears the IP address.
no primary dns	Clears the name of the primary DNS server.
no secondary dns	Clears the name of the secondary DNS server.
primary dns <*IP address*>	Sets the IP address of the primary DNS server.
secondary dns <*IP address*>	Sets the IP address of the secondary DNS server.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Show interface status
state disable	Disables the interface.
state enable	Enables the interface.
write	Stores the current configuration in permanent memory.
ip (config-ip) level commands	
clrscrn	Clears the screen.
default ip time to live	Restores the default IP time to live.
default multicast time to live	Restores the default IP multicast time to live, which is one hop.
exit	Exits to the configuration level.
ip time to live <*hops*>	Sets the IP time to live, known by SNMP as "ipDefaultTTL". <hops> = number of hops that a typical IP packet is allowed to live.
multicast time to live <*hops*>	Sets the IP multicast time to live. <hops> = number of hops that a multicast IP packet is allowed to live.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
line 1 (line:1) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <*bits per second*>	Sets the line speed. <bits per second> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <*string*>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
command mode signon message <*string*>	Sets a sign-on message that is sent from the serial port when the device boots and when the line is in command mode.

	<string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
command mode wait time <*milliseconds*>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default interface	Restores the default interface type to this line.
default parity	Restores the default of no parity.
default protocol	Restores the default protocol on the line.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <*milliseconds*>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
interface rs232	Sets the line interface to RS232.
interface rs485 full-duplex	Sets the line interface to RS485 in full-duplex mode.
interface rs485 half-duplex	Sets the line interface to RS485 in half-duplex mode.
interface usb-cdc-acm	Sets the line interface to USB-CDC-ACM mode.
kill session	Kills command mode session on the Line
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
name <*text*>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.
show history	Displays the last 20 commands entered during the current CLI session.

show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
termination disable	Refrains from terminating the line.
termination enable	Enables 120 ohm line termination in RS485 half-duplex mode.
threshold <*bytes*>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <*control*>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
xon char <*control*>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
line 2 (line:2) level commands	
auto show statistics	Continuously displays line statistics.
baud rate <*bits per second*>	Sets the line speed. <bits per second> = the speed. Standard speeds include 1200, 2400, 4800, 9600, 19200, and so on.
clear line counters	Sets the serial counters to zero.
clrscrn	Clears the screen.
command mode always	Sets the current line to always be in command mode.
command mode echo serial string disable	Disables user-defined serial boot string to be echoed in the CLI.
command mode echo serial string enable	Enables user-defined serial boot string to be echoed in the CLI.
command mode serial string	Enables user to enter a custom string at boot time to enter command mode.
command mode serial string <*string*>	Sets a string that can be entered at boot time to enter command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF. Within {} specify decimal milliseconds time delay.
command mode signon message <*string*>	Sets a sign-on message that is sent from the serial port

	when the device boots and when the line is in command mode. <string> = text with possible binary characters. Within [] use binary decimal up to 255 or hex up to 0xFF.
command mode wait time <*milliseconds*>	Sets boot-up wait time for command mode serial string. <milliseconds> = wait time.
configure current settings	Configures line with the current value of settings.
data bits 7	Uses seven bits for data on the line.
data bits 8	Uses eight bits for data on the line.
default baud rate	Restores the default speed of 9600 bits per second.
default data bits	Restores the default of eight data bits.
default flow control	Restores the default of no flow control.
default interface	Restores the default interface type to this line.
default parity	Restores the default of no parity.
default protocol	Restores the default protocol on the line.
default stop bits	Restores the default of one stop bit.
default threshold	Restores the factory default threshold.
default xoff char	Restores the default xoff character on this line.
default xon char	Restores the default xon character on this line.
exit	Exits to the enable level
flow control hardware	Uses hardware (RTS/CTS) flow control on the line.
flow control none	Does not provide flow control on the line.
flow control software	Uses software (xon/xoff characters) flow control on the line.
gap timer <*milliseconds*>	Sets the gap timer in milliseconds. If some data has been received, it will be forwarded after this time since the last character.
interface rs232	Sets the line interface to RS232.
interface rs485 full-duplex	Sets the line interface to RS485 in full-duplex mode.
interface rs485 half-duplex	Sets the line interface to RS485 in half-duplex mode.
interface usb-cdc-acm	Sets the line interface to USB-CDC-ACM mode.
kill session	Kills command mode session on the Line
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
name <*text*>	Sets the name for this line.
no clear line counters	Restores the serial counters to the aggregate values.
no command mode	Disables command mode for the current line.
no command mode signon message	Clears the signon message displayed at boot time and when entering command mode.
no gap timer	Removes the gap timer, so forwarding depends on the line speed.
no name	Removes the name of this line.
parity even	Uses a parity bit on the line for even parity.
parity none	Does not use a parity bit on the line.
parity odd	Uses a parity bit on the line for odd parity.
protocol none	Uses no protocol on the line.
protocol tunnel	Applies tunnel protocol on the line.
reassert	Asserts line status with current configured values.
show	Displays the current status.
show command mode	Shows the command mode settings for the current line.

show history	Displays the last 20 commands entered during the current CLI session.
show line	Displays the current configuration.
show statistics	Shows the line statistics.
state disable	Disables the line so data cannot be sent/received.
state enable	Enables the line so data can be sent/received.
stop bits 1	Uses one stop bit after data on the line.
stop bits 2	Uses two stop bits after data on the line.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
termination disable	Refrains from terminating the line.
termination enable	Enables 120 ohm line termination in RS485 half-duplex mode.
threshold <*bytes*>	Sets the threshold in bytes. After this many bytes are received, they are forwarded without delay.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
xoff char <*control*>	Sets the xoff character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
xon char <*control*>	Sets the xon character for use with software flow control on this line. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
link (config-wlan:wlan0) level commands	
active channel scan time <*milliseconds*>	Sets the active channel scan time in milliseconds.
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
cancel wps	Cancels wi-fi protected setup operation.
choice <*instance*>	Enters the next lower level. Specify the instance for the next lower level.
clrscrn	Clears the screen.
debugging level debug	Sets the WLAN debugging level to Debug.
debugging level dump	Sets the WLAN debugging level to Dump, the most verbose option.
debugging level error	Sets the WLAN debugging level to Error, which shows only errors.
debugging level info	Sets the WLAN debugging level to Info.
debugging level warning	Sets the WLAN debugging level to Warning.
default active channel scan time	Restores the default active channel scan time.
default debugging level	Sets the WLAN debugging level to its default value, Info.

default out of range scan interval	Restores the default value to the out-of-range scan interval (30 sec).
default passive channel scan time	Restores the default passive channel scan time.
default radio band selection	Sets the radio band selection to its default value, Dual.
default rssi delta	Restores the RSSI delta value to the default value (24 dBm).
exit	Exit back to interface configuration level
out of range scan interval <*seconds*>	This setting determines the interval (in seconds) between scans for access points to which the unit might roam. This setting only applies when roaming is enabled. Note: The more frequent the scans, the greater the impact on data throughput.
passive channel scan time <*milliseconds*>	Sets the passive channel scan time in milliseconds.
radio band selection 2.4 ghz only	Sets the radio band selection to 2.4 GHz Only.
radio band selection 5 ghz only	Sets the radio band selection to 5 GHz Only.
radio band selection dual	Sets the radio band selection to Dual.
roam status	Show roaming status
roaming disable	Disables roaming.
roaming enable	Enables roaming to other Access Points with the same SSID.
rssi delta <*dBm*>	Sets the RSSI delta value.
scan <*ssid*>	Scan the radio environment for networks.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show wps information	Show the configuration received by wi-fi protected setup.
show wps information with secrets	Show the configuration received by wi-fi protected setup with secrets.
show wps status	Show status of WPS operation.
start wps	Starts wi-fi protected setup operation.
status	Show link status
write	Stores the current configuration in permanent memory.
link (config-ethernet:eth0) level commands	
clrscrn	Clears the screen.
default duplex	Restores the default duplex setting, which is auto.
default speed	Restores the default speed setting, which is auto-negotiate.
duplex auto	Sets duplex mode to auto.
duplex full	Sets duplex mode to full.
duplex half	Sets duplex mode to half.
exit	Exit back to interface configuration level
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
speed 10	Sets the speed of the Ethernet link to 10 Mbps.
speed 100	Sets the speed of the Ethernet link to 100 Mbps.
speed auto	Sets the speed of the Ethernet link to auto-negotiate.
write	Stores the current configuration in permanent memory.
log (config-diagnostics-log) level commands	
clrscrn	Clears the screen.
default max length	Restores the factory default maximum Log file size.

default output	Restores the default log output, which is disable.
exit	Exits to the next higher level.
max length *<Kbytes>*	Sets the maximum size in Kbytes for the Log file.
output disable	Disables log output.
output filesystem	Enables log to filesystem.
output line *<number>*	Enables log to serial line.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:2) level commands	
clrscrn	Clears the screen.
connect string *<text>*	Sets the CONNECT string used in modem emulation. <string> = connect string.
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.
display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
modem (tunnel-modem:1) level commands	
clrscrn	Clears the screen.
connect string *<text>*	Sets the CONNECT string used in modem emulation. <string> = connect string.
default incoming connection	Default disables incoming network connections.
default response type	Default uses text type responses.

display remote ip disable	The incoming RING has nothing following it.
display remote ip enable	The incoming RING is followed by the IP address of the caller.
echo commands disable	Does not echo modem commands.
echo commands enable	Echoes modem commands.
echo pluses disable	Does not echo the +++ characters when entering modem command mode.
echo pluses enable	Echoes the +++ characters when entering modem command mode.
error unknown commands disable	Returns OK on unknown AT commands.
error unknown commands enable	Returns an error upon unknown AT commands.
exit	Returns to the tunnel level.
incoming connection automatic	Automatically answer incoming network connections.
incoming connection disabled	Disable incoming network connections.
incoming connection manual	Wait for an ATA command before answering an incoming network connection.
no connect string	Removes optional CONNECT string information for modem emulation.
reassert	Asserts tunnel modem status with current configured values.
response type numeric	Uses numeric type responses.
response type text	Uses text type responses.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays tunnel modem status.
verbose response disable	Does not send Modem Response Codes.
verbose response enable	Sends Modem Response Codes out on the Serial Line.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:2) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <*control*>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.

show history	Displays the last 20 commands entered during the current CLI session.
threshold <*bytes*>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <bytes> = number of bytes in the threshold.
timeout <*milliseconds*>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.
trailing character <*control*>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
packing (tunnel-packing:1) level commands	
clrscrn	Clears the screen.
default packing mode	Sets to default packing mode, which is "Disable"
default send character	Removes the send character for packing mode.
default threshold	Restores the default threshold.
default timeout	Restores the default packing mode timeout.
exit	Returns to the tunnel level.
no trailing character	Removes the trailing character for packing mode.
packing mode disable	Disables packing. Data is sent to the network when received.
packing mode send character	Sets packing mode to accumulate data and transmit it upon receiving the configured send character on the line (serial port).
packing mode timeout	Sets packing mode to accumulate data and transmit it after a specified amount of time (timeout).
send character <*control*>	Sets the send character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
threshold <*bytes*>	Sets the threshold (byte count). If the queued data reaches this threshold then the data will be sent. <bytes> = number of bytes in the threshold.
timeout <*milliseconds*>	Sets the timeout value for packing mode in milliseconds. <milliseconds> = timeout value, in milliseconds.
trailing character <*control*>	Sets the trailing character for packing mode. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:2) level commands	
clrscrn	Clears the screen.

exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <*text*>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
password (tunnel-accept-password:1) level commands	
clrscrn	Clears the screen.
exit	Exits to the next higher level.
no password	Removes the password so connections will be accepted unchallenged.
password <*text*>	Sets the password required on the network side of the tunnel to begin a connection.
prompt disable	Inhibits any prompting for password on the network side of the tunnel.
prompt enable	Sets up so a user on the network side of the tunnel will be prompted for a password.
show	Shows the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
query port (config-query_port) level commands	
clear counters	Zeros Query Port counters
clrscrn	Clears the screen.
exit	Returns to the config level.
no clear counters	Unzeros Query Port counters
show	Displays statistics and information about the query port.
show history	Displays the last 20 commands entered during the current CLI session.
state disable	Disables response to 77FE requests.
state enable	Permits response to 77FE requests.
write	Stores the current configuration in permanent memory.
root level commands	
clrscrn	Clears the screen.
enable	Enters the enable level.
exit	Exit from the system
ping <*host*>	Ping destination continuously with 5 second timeout
ping <*host*> <*count*>	Ping destination n times with 5 second timeout
ping <*host*> <*count*> <*timeout*>	Ping destination n times with x timeout (in seconds)
show	Show system information
show history	Displays the last 20 commands entered during the current

	CLI session.
trace route <*host*>	Trace route to destination
trace route <*host*> <*protocol*>	Trace route to destination using TCP, ICMP, or UDP
rss (config-rss) level commands	
clear rss	Clear the RSS Feed data
clrscrn	Clears the screen.
default max entries	Restores the default number of RSS feed entries.
exit	Exits to the configuration level.
feed disable	Disables RSS feed.
feed enable	Enables RSS feed.
max entries <*number*>	Sets the maximum number of RSS feed entries.
persist disable	Disables RSS feed data persistence.
persist enable	Enables RSS feed data persistence.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Display the RSS Feed status
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:2) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
serial (tunnel-serial:1) level commands	
clrscrn	Clears the screen.
default dtr	Restores default DTR control, asserted while connected.
dtr asserted while connected	Asserts DTR whenever a connect or accept mode tunnel connection is active.
dtr continuously asserted	Asserts DTR regardless of any connections.
dtr truport	Asserts DTR to match remote DSR when connected via Telnet.
dtr unasserted	Does not assert DTR.
exit	Returns to the tunnel level.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
server (ssh-server) level commands	
authorized user <*username*> <*password*>	Sets authorized username, password, and optionally RSA and/or DSA public keys
clrscrn	Clears the screen.

delete all authorized users	Removes all authorized users
delete authorized user <*username*>	Remove an authorized user
exit	Exits to the ssh level.
host generate dsa 1024	Generate DSA public and private keys
host generate dsa 512	Generate DSA public and private keys
host generate dsa 768	Generate DSA public and private keys
host generate rsa 1024	Generate RSA public and private keys
host generate rsa 512	Generate RSA public and private keys
host generate rsa 768	Generate RSA public and private keys
host keys	Sets RSA or DSA public and/or private keys
no host dsa	Removes DSA public and private keys
no host rsa	Removes RSA public and private keys
show	Show SSH Server settings
show authorized user <*username*>	Show information for an authorized user
show history	Displays the last 20 commands entered during the current CLI session.
show host dsa	Show full DSA public key
show host rsa	Show full RSA public key
write	Stores the current configuration in permanent memory.
smtp (config-smtp) level commands	
clrscrn	Clears the screen.
default relay port	Restores the SMTP relay port to its default.
exit	Exits to the configuration level.
no relay address	Removes the SMTP relay address.
relay address <*text*>	Sets an SMTP relay address to direct all outbound email messages through a mail server.
relay port <*number*>	Sets the SMTP relay port.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
ssh (ssh) level commands	
client	Enters the SSH Client configuration level.
clrscrn	Clears the screen.
exit	Exits to the enable level.
server	Enters the SSH Server configuration level.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
ssh (config-cli-ssh) level commands	
clrscrn	Clears the screen.
default max sessions	Restores the default maximum allowed concurrent incoming SSH sessions.
default port	Restores the default local port to the SSH server.
exit	Exits to the CLI level.
max sessions <*number*>	Sets the maximum allowed concurrent incoming SSH sessions. <number> = number of sessions.
port <*number*>	Sets the local port that the SSH server uses.

	<number> = local port number.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the SSH server statistics.
state disable	Disables the SSH Server.
state enable	Enables the SSH Server.
write	Stores the current configuration in permanent memory.
ssl (ssl) level commands	
clrscrn	Clears the screen.
credentials	Enters the SSL credentials configuration level.
exit	Exits to the enable level.
show history	Displays the last 20 commands entered during the current CLI session.
trusted authorities	Enters the SSL configuration level.
write	Stores the current configuration in permanent memory.
syslog (config-syslog) level commands	
clrscrn	Clears the screen.
default remote port	Restores the default syslog remote port.
default severity log level	No logging.
exit	Returns to the config level.
host <*text*>	Sets the address of the syslog recipient. <text> = IP address or name of the host.
no host	Removes the address of the syslog recipient.
remote port <*number*>	Sets the syslog remote port. <number> = number of the remote port used when making a syslog connection.
severity log level alert	Log only Alert and more severe events.
severity log level critical	Log only Critical and more severe events.
severity log level debug	Log all events.
severity log level emergency	Log only Emergency events.
severity log level error	Log only Error and more severe events.
severity log level information	Log only Information and more severe events.
severity log level none	No logging.
severity log level notice	Log only Notice and more severe events.
severity log level warning	Log only Warning and more severe events.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the syslog statistics.
state disable	Disables syslog logging.
state enable	Enables syslog logging.
write	Stores the current configuration in permanent memory.
telnet (config-cli-telnet) level commands	
authentication disable	No password required for Telnet users.
authentication enable	Challenges the Telnet user with a password.
clrscrn	Clears the screen.
default max sessions	Restores the default maximum allowed concurrent incoming Telnet sessions.
default port	Restores the default local port to the Telnet server.

exit	Exits to the CLI level.
max sessions <*number*>	Sets the maximum allowed concurrent incoming Telnet sessions. <number> = number of sessions.
port <*number*>	Sets the local port that the Telnet server uses. <number> = local port number.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	Displays the Telnet statistics.
state disable	Disables the Telnet Server.
state enable	Enables the Telnet Server.
write	Stores the current configuration in permanent memory.
terminal 1 (config-terminal:1) level commands	
break duration <*milliseconds*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*control*>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be con-

	figured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
terminal 2 (config-terminal:2) level commands	
break duration <*milliseconds*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*control*>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.

write	Stores the current configuration in permanent memory.
terminal network (config-terminal:network) level commands	
break duration <*milliseconds*>	Sets how long a break should last when it is being sent to the line. <milliseconds> = number of milliseconds.
clrscrn	Clears the screen.
default break duration	Restores the break duration to the default value (500 ms).
default terminal type	Sets the default terminal type, "UNKNOWN".
echo disable	Disables echoing of characters received on the line back to the line.
echo enable	Enables echoing of characters received on the line back to the line.
exit	Exits to the configuration level.
exit connect menu disable	On the login connect menu, removes the menu item allowing the user to exit to the CLI.
exit connect menu enable	On the login connect menu, inserts the menu item allowing the user to exit to the CLI.
line <*line*>	Enters the line level. <line> = number of the line (serial port) to be configured.
login connect menu disable	Disables the login connect menu, so a user will get the CLI immediately after logging in.
login connect menu enable	Enables the login connect menu, so a user will get the menu rather than the CLI immediately after logging in.
no send break	Removes the configured send break character.
preview connect menu	Shows the layout of the connect menu with current settings.
send break <*control*>	Sets the optional send break character. <text> = the character. The character may be input as text, control, decimal, or hex. A control character has the form <control>C. A decimal value character has the form \99. A hex value character has the form 0xFF.
show	Displays the current configuration.
show history	Displays the last 20 commands entered during the current CLI session.
terminal <*line*>	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
terminal type <*text*>	Sets the terminal type.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
trusted authorities (ssl-auth) level commands	
add	Adds an Authority Certificate.
clrscrn	Clears the screen.
exit	Exits to the ssl level.
no intermediate authority <*cert*>	Removes an Intermediate Authority Certificate.

	<cert> = index displayed by "show authority" command.
no trusted authority *<cert>*	Removes a Trusted Authority Certificate. <cert> = index displayed by "show authority" command.
show	Displays Authority Certificate Information.
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
tunnel 1 (tunnel:1) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line *<line>*	Enters the line level. <line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal *<line>*	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be configured.
terminal network	Enters the configure-terminal level for the network.
tunnel *<line>*	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
tunnel 2 (tunnel:2) level commands	
accept	Enters the accept level for this tunnel.
auto show statistics	show connection statistics
clear counters	Zeros all tunnel counters
clrscrn	Clears the screen.
connect	Enters the connect level for this tunnel.
disconnect	Enters the disconnect level for this tunnel.
exit	Exits to the enable level.
line *<line>*	Enters the line level. <line> = number of the line (serial port) to be configured.
modem	Enters the modem level for this tunnel.
no clear counters	Unzeros all tunnel counters
packing	Enters the packing level for this tunnel.
serial	Enters the serial level for this tunnel.
show history	Displays the last 20 commands entered during the current CLI session.
show statistics	show connection statistics
terminal *<line>*	Enters the configure-terminal level. <line> = number of the terminal line (serial port) to be con-

	figured.
terminal network	Enters the configure-terminal level for the network.
tunnel <*line*>	Enters the tunnel level. <line> = number of the tunnel line (serial port) to be configured.
write	Stores the current configuration in permanent memory.
vip (config-vip) level commands	
auto show counters	Displays VIP counters continuously.
auto show status	Displays VIP status continuously.
clear counters	Sets the VIP counters to zero.
clrscrn	Clears the screen.
exit	Exits to the configuration level.
no clear counters	Restores the VIP counters to the aggregate values.
show	Displays the current configuration.
show counters	Displays the VIP counters.
show history	Displays the last 20 commands entered during the current CLI session.
show status	Displays the VIP status.
state disable	Disables use of Virtual IP (VIP) addresses.
state enable	Enables use of Virtual IP (VIP) addresses.
write	Stores the current configuration in permanent memory.
wlan profiles (config-profiles) level commands	
apply wlan	Try out WLAN settings without saving them to Flash. If the settings do not work, when you reboot the device, it will still have the original settings.
clrscrn	Clears the screen.
create <*profile name*>	Create a new profile name
delete <*profile name*>	Delete existing profile by name
edit <*profile name*>	View or edit an existing profile
exit	Exits to the config level.
show	Show existing profile names
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
xml (xml) level commands	
clrscrn	Clears the screen.
exit	Exits to the enable level.
secret xcr dump	Dump XML configuration containing secrets to the console
secret xcr dump <*group list*>	Dump specified XML configuration containing secrets to the console
secret xcr export <*file*>	Save XML configuration containing secrets to a file
secret xcr export <*file*> <*group list*>	Save specified XML configuration containing secrets to a local file
show history	Displays the last 20 commands entered during the current CLI session.
write	Stores the current configuration in permanent memory.
xcr dump	Dump XML configuration to the console
xcr dump <*group list*>	Dump specified XML configuration to the console
xcr export <*file*>	Save XML configuration to a file
xcr export <*file*> <*group list*>	Save specified XML configuration to a local file

xcr import <*file*>	Load XML configuration from a local file
xcr import <*file*> <*group list*>	Load specified XML configuration from a local file
xcr list	List XML Configuration Record groups to the console
xsr dump	Dump XML Status Records to the console
xsr dump <*group list*>	Dump specified XML Status Records to the console
xsr export <*file*>	Save XML Status Record to a file
xsr export <*file*> <*group list*>	Save specified XML Status Record to a local file
xsr list	List XML Status Record groups to the console